

日 本 国 特 許 庁

26.12.00

PATENT OFFICE  
JAPANESE GOVERNMENT

JP00/9283

REC'D 02 MAR 2001

WIPQ PCI

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日

Date of Application:

2000年 2月15日

出 願 番 号

Application Number:

特願2000-037134

出 願 人

Applicant(s):

松下電子工業株式会社

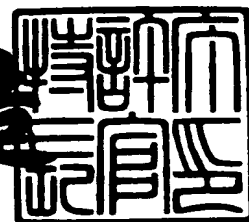
BEST AVAILABLE COPY

PRIORITY  
DOCUMENTSUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2001年 2月 9日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2001-3005452

特 2000-037134

【書類名】 特許願  
【整理番号】 2925010067  
【提出日】 平成12年 2月15日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G06F 17/00

【発明者】

【住所又は居所】 大阪府高槻市幸町1番1号 松下電子工業株式会社内

【氏名】 玉井 誠一郎

【特許出願人】

【識別番号】 000005843

【氏名又は名称】 松下電子工業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【選任した代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9810106

【プルーフの要否】 要

出証特2001-300545

【書類名】 明細書

【発明の名称】 情報記憶媒体、非接触 IC タグ、アクセス装置、アクセスシステム、ライフサイクル管理システム、入出力方法及びアクセス方法

【特許請求の範囲】

【請求項 1】 不揮発性メモリを有し、電波を用いて非接触に読み書き可能な

情報記憶媒体であって、

複数の記憶領域を有する記憶手段と、

各記憶領域を識別する識別子を格納している格納手段と、

外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、

受信した前記アクセス識別子が前記格納手段に格納されている識別子のいずれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、

受信したアクセス情報に基づいて、前記アクセス識別子により識別される記憶領域へのアクセスを行う入出力手段と

を備えることを特徴とする情報記憶媒体。

【請求項 2】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触 IC タグであって、

前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、

前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、

外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、

受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信する

アクセス情報受信手段と、

受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段と

を備えることを特徴とする非接触ICタグ。

【請求項3】 前記秘密受信手段は、

第1認証子を生成し、生成した第1認証子を前記アクセス装置へ出力する認証子出力手段と、

前記アクセス識別子を暗号化鍵として用いて、出力した前記第1認証子に暗号アルゴリズムが施されて生成された第2認証子を前記アクセス装置から取得する取得手段と、

前記複数のステージ識別子を暗号化鍵として用いて、生成した前記第1認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第3認証子を生成する暗号手段とを含み、

前記判断手段は、取得した第2認証子が生成した複数の第3認証子のうちのいずれか1個と一致するか否かを判断し、一致する場合に、受信した前記アクセス識別子が前記識別子記憶手段に格納されているステージ識別子のいずれかと一致すると判断し、

前記入出力手段は、前記アクセス識別子により識別されるステージ記憶領域として、前記第2認証子に一致する第3認証子を生成する際に暗号化鍵として用いられたステージ識別子により識別されるステージ記憶領域へのアクセスを行うことを特徴とする請求項2記載の非接触ICタグ。

【請求項4】 前記認証子出力手段は、ランダムに第1認証子を生成することを特徴とする請求項3記載の非接触ICタグ。

【請求項5】 前記秘密受信手段は、

時分割多重された通信チャネルのうち、1個の通信チャネルを選択するチャネル選択手段と、

選択された前記通信チャネルを介して、アクセス識別子を秘密に受信する識別子受信手段と

を含むことを特徴とする請求項4に記載の非接触ICタグ。

【請求項6】 前記チャネル選択手段は、時分割多重された通信チャネルのうち、1個の通信チャネルをランダムに選択すること

ことを特徴とする請求項5に記載の非接触ICタグ。

【請求項7】 前記記憶手段は、さらに、共有識別子により識別される共有記憶領域を有し、

前記識別子記憶手段は、さらに、前記共有識別子を記憶しており、

前記判断手段は、さらに、受信した前記アクセス識別子が前記識別子記憶手段に記憶されている共有識別子と一致するか否かを判断し、

前記アクセス情報受信手段は、さらに、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信し、

前記入出力手段は、さらに、受信したアクセス情報に基づいて、前記アクセス識別子により識別される共有記憶領域へのアクセスを行う

ことを特徴とする請求項2に記載の非接触ICタグ。

【請求項8】 前記非接触ICタグが有する不揮発性メモリは、ヒューズメモリである

ことを特徴とする請求項2に記載の非接触ICタグ。

【請求項9】 入院から退院に至るまでの病院の療養サイクルにおける複数のステージを経由する入院患者に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、

前記療養サイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、

前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、

外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、

受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、

受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段と  
を備えることを特徴とする非接触ICタグ。

【請求項10】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する高級ブランド品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、

前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、

前記複数のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、

外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、

受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、

受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段と  
を備えることを特徴とする非接触ICタグ。

【請求項11】 不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別される複数の記憶領域を有し、電波を用いて非接触に読み書き可能な情報記憶媒体に対して情報を送受信するアクセス装置であって、

アクセス識別子を記憶している識別子記憶手段と、

前記アクセス識別子を暗号を用いて秘密に前記情報記憶媒体に対して送信する秘密送信手段と、

前記情報記憶媒体により、秘密に送信した前記アクセス識別子が前記情報記憶媒体が有する複数の記憶領域うちの1個の記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段と

を備えることを特徴とするアクセス装置。

【請求項 12】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触 IC タグに対して情報を送受信するアクセス装置であって、

アクセス識別子を記憶している識別子記憶手段と、

前記アクセス識別子を暗号を用いて秘密に前記非接触 IC タグに対して送信する秘密送信手段と、

前記非接触 IC タグにより、秘密に送信した前記アクセス識別子が前記非接触 IC タグが有する複数のステージ記憶領域うちの 1 個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段と

を備えることを特徴とするアクセス装置。

【請求項 13】 前記非接触 IC タグは、前記複数のステージ記憶領域をそれぞれ識別するステージ識別子を記憶しており、

前記秘密送信手段は、

前記非接触 IC タグから第 1 認証子を受信する認証子受信手段と、

前記アクセス識別子を暗号鍵として用いて、受信した前記第 1 認証子に暗号アルゴリズムを施して第 2 認証子を生成し、生成した第 2 認証子を前記非接触 IC タグへ出力する認証子出力手段とを備え、

前記アクセス情報送信手段は、前記非接触 IC タグにより、前記複数のステージ識別子を暗号化鍵として用いて、前記第 1 認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第 3 認証子が生成され、出力された前記第 2 認証子が生成した複数の第 3 認証子のうちのいずれか 1 個と一致するか否か判断され、一致する場合に、前記アクセス識別子が前記複数のステージ記憶領域うちの 1 個のステージ記憶領域を正しく識別すると判断されるときに、さらにアクセス情報を送信する

ことを特徴とする請求項 12 記載のアクセス装置。

【請求項 14】 生産から廃棄に至るまでのライフサイクルにおける複数のス

テージを流通する物品に付され、不揮発性メモリにより構成されライフサイクルを構成するステージ数と同数のステージ記憶領域を備え、電波を用いて非接触に読み書き可能な非接触 I C タグと前記非接触 I C タグに対して情報を送受信するアクセス装置とから構成されるアクセスシステムであって、

請求項 2 記載の非接触 I C タグと、

請求項 1 2 記載のアクセス装置と

から構成されることを特徴とするアクセスシステム。

【請求項 1 5】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成されライフサイクルを構成するステージ数と同数のステージ記憶領域を備え、電波を用いて非接触に読み書き可能な非接触 I C タグと前記非接触 I C タグに対して情報を送受信するアクセス装置とから構成されるアクセスシステムであって、

請求項 3 記載の非接触 I C タグと、

請求項 1 3 記載のアクセス装置と

から構成されることを特徴とするアクセスシステム。

【請求項 1 6】 不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触 I C タグが付された物品が、生産から廃棄に至るまでの複数ステージを流通する物品ライフサイクルにおいて、ステージ毎に設けられたアクセス装置により前記非接触 I C タグにアクセスすることにより、前記物品を管理するライフサイクル管理システムであって、

請求項 2 記載の非接触 I C タグと、

請求項 1 2 記載のアクセス装置とを含み、

ステージ毎に設けられたアクセス装置により、前記非接触 I C タグが有し、当該ステージに対応する 1 のステージ記憶領域にのみアクセスすることにより、前記物品を管理する

ことを特徴とするライフサイクル管理システム。

【請求項 1 7】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能であり、前記ライフサイクルを構成するステージ数と同数のステー



ジ記憶領域を有する記憶手段と前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段とを備える非接触ＩＣタグにより用いられる入出力方法であって、

外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信ステップと、

受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断ステップと、

一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信ステップと、

受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力ステップと  
を含むことを特徴とする入出力方法。

【請求項１８】 生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触ＩＣタグに対して情報を送受信し、アクセス識別子を記憶している識別子記憶手段を備えるアクセス装置により用いられるアクセス方法であって、

前記アクセス識別子を暗号を用いて秘密に前記非接触ＩＣタグに対して送信する秘密送信ステップと、

前記非接触ＩＣタグにより、秘密に送信した前記アクセス識別子が前記非接触ＩＣタグが有する複数個のステージ記憶領域うちの１個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信ステップと

を含むことを特徴とするアクセス方法。

#### 【発明の詳細な説明】

##### 【０００１】

##### 【発明の属する技術分野】

本発明は、非接触ＩＣタグが付された対象が複数ステージを流通する場合にお

いて、前記非接触 I C タグにアクセスすることにより、前記対象を管理する技術に関する。

#### 【 0 0 0 2 】

##### 【従来の技術】

物品の生産から廃棄に至るまでのいわゆるライフサイクルにおいて、製品の稼働状況や履歴情報を収集し、この情報を利用して物品を管理するアイデアが提案されている。

例えば、特開平 1 0 - 2 2 2 5 6 8 号公報によると、ライフサイクル全体での低コスト化を実現するために、製品の製造時、使用時、メンテナンス時に型番・製造番号などの識別情報、材質情報、稼働情報、エラー情報、メンテナンス情報を、各製品、部品毎に入力し、入力された情報を記憶し、記憶された情報を読み出して、製造、メンテナンス、回収、中古販売などの各ステージで判断し、評価するシステムが開示されている。

#### 【 0 0 0 3 】

また、特開平 1 1 - 1 2 0 3 0 8 号公報によると、製品機器に関する履歴情報が製品と一体的に記憶されるようにした履歴情報記憶装置が開示されている。

#### 【 0 0 0 4 】

##### 【発明が解決しようとする課題】

しかしながら、従来技術によると、製品に関する情報を製品に付加し、製品と情報とを一体として、ライフサイクルを構成する各ステージを流通させることができ、製造、メンテナンス、回収、中古販売などの各ステージで製品に関する情報を共有し自由に利用することができるものの、製品に付加された情報は誰でも利用できるのも、各業者は、秘密の情報を製品に付加することができないという問題点がある。このため、製品と製品に関する情報とを一体として、ライフサイクルを流通させる技術が現実には普及しない原因の一つとなっている。

#### 【 0 0 0 5 】

本発明は、上記の問題点を解決するために、情報記憶媒体又は非接触 I C タグが付された対象が複数ステージを流通する場合において、ステージ毎の秘密の情報を記憶することができる情報記憶媒体及び非接触 I C タグ、前記非接触 I C タ

グに対してステージ毎に秘密に情報を読み書きすることができるアクセス装置、非接触ＩＣタグとアクセス装置とから構成されるアクセスシステム、非接触ＩＣタグとステージ毎に設けられるアクセス装置とを含むライフサイクル管理システム、非接触ＩＣタグで用いられる入出力方法及びアクセス装置で用いられるアクセス方法を提供することを目的とする。

#### 【 0 0 0 6 】

##### 【課題を解決するための手段】

上記目的を達成するために、本発明は、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な情報記憶媒体であって、複数の記憶領域を有する記憶手段と、各記憶領域を識別する識別子を格納している格納手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記格納手段に格納されている識別子のいずれかと一致するか否かを判断する判断手段と、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別される記憶領域へのアクセスを行う入出力手段とを備えることを特徴とする。

#### 【 0 0 0 7 】

また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ＩＣタグであって、前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段とを備えることを特徴とする。

#### 【 0 0 0 8 】

ここで、前記秘密受信手段は、第 1 認証子を生成し、生成した第 1 認証子を前記アクセス装置へ出力する認証子出力手段と、前記アクセス識別子を暗号化鍵として用いて、出力した前記第 1 認証子に暗号アルゴリズムが施されて生成された第 2 認証子を前記アクセス装置から取得する取得手段と、前記複数のステージ識別子を暗号化鍵として用いて、生成した前記第 1 認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第 3 認証子を生成する暗号手段とを含み、前記判断手段は、取得した第 2 認証子が生成した複数の第 3 認証子のうちのいずれか 1 個と一致するか否かを判断し、一致する場合に、受信した前記アクセス識別子が前記識別子記憶手段に格納されているステージ識別子のいずれかと一致すると判断し、前記入出力手段は、前記アクセス識別子により識別されるステージ記憶領域として、前記第 2 認証子に一致する第 3 認証子を生成する際に暗号化鍵として用いられたステージ識別子により識別されるステージ記憶領域へのアクセスを行うように構成してもよい。

## 【 0 0 0 9 】

ここで、前記認証子出力手段は、ランダムに第 1 認証子を生成するように構成してもよい。

ここで、前記秘密受信手段は、時分割多重された通信チャネルのうち、1 個の通信チャネルを選択するチャネル選択手段と、選択された前記通信チャネルを介して、アクセス識別子を秘密に受信する識別子受信手段とを含むように構成してもよい。

## 【 0 0 1 0 】

ここで、前記チャネル選択手段は、時分割多重された通信チャネルのうち、1 個の通信チャネルをランダムに選択するように構成してもよい。

ここで、前記記憶手段は、さらに、共有識別子により識別される共有記憶領域を有し、前記識別子記憶手段は、さらに、前記共有識別子を記憶しており、前記判断手段は、さらに、受信した前記アクセス識別子が前記識別子記憶手段に記憶されている共有識別子と一致するか否かを判断し、前記アクセス情報受信手段は、さらに、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信し、前記入出力手段は、さらに、受信したアクセス情報に基づいて、前記ア

アクセス識別子により識別される共有記憶領域へのアクセスを行うように構成してもよい。

【0011】

また、本発明は、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別される複数個の記憶領域を有し、電波を用いて非接触に読み書き可能な情報記憶媒体に対して情報を送受信するアクセス装置であって、アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子を暗号を用いて秘密に前記情報記憶媒体に対して送信する秘密送信手段と、前記情報記憶媒体により、秘密に送信した前記アクセス識別子が前記情報記憶媒体が有する複数個の記憶領域うちの1個の記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備えることを特徴とする。

【0012】

また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触ICタグに対して情報を送受信するアクセス装置であって、アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子を暗号を用いて秘密に前記非接触ICタグに対して送信する秘密送信手段と、前記非接触ICタグにより、秘密に送信した前記アクセス識別子が前記非接触ICタグが有する複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備えることを特徴とする。

【0013】

ここで、前記非接触ICタグは、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶しており、前記秘密送信手段は、前記非接触ICタグから第1認証子を受信する認証子受信手段と、前記アクセス識別子を暗号鍵として用いて、受信した前記第1認証子に暗号アルゴリズムを施して第2認証子を生成し、生成した第2認証子を前記非接触ICタグへ出力する認証子出力手段とを備え、前記アクセス情報送信手段は、前記非接触ICタグにより、前記複数の

ステージ識別子を暗号化鍵として用いて、前記第 1 認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第 3 認証子が生成され、出力された前記第 2 認証子が生成した複数の第 3 認証子のうちのいずれか 1 個と一致するかどうか判断され、一致する場合に、前記アクセス識別子が前記複数個のステージ記憶領域うちの 1 個のステージ記憶領域を正しく識別すると判断されるときに、さらにアクセス情報を送信するように構成してもよい。

【 0 0 1 4 】

### 【発明の実施の形態】

#### 1 第 1 の実施の形態

本発明の 1 の実施の形態としてのライフサイクル管理システム 1 0 について説明する。

##### 1. 1 製品のライフサイクル

生産業者は、生産工場において、部品を加工し、組み立てて、製品（物品）を生産し、生産した製品を出荷する。物流業者は、出荷された製品を販売業者へ輸送する。販売業者は、製品を需要者に販売し、需要者は、その製品を使用する。サービス業者は、需要者により使用されている製品を補修・修理する。回収リサイクル業者は、長年使用された製品を解体、廃棄する。解体された製品の一部分は、再度製品を加工する際に部品として使用される。

【 0 0 1 5 】

こうして、製品は、図 1 に示すように、生産 1、物流 2、販売 3、サービス 4、回収リサイクル 5 の各ステージを経て流通し、その一生を終える。製品の生産から廃棄・回収に至るまでを、製品のライフサイクル 6 と呼ぶ。

生産業者は、その生産の 1 工程において、1 個の無線 IC タグ（後述する）を製品に付す。例えば、テレビ受像機が生産業者は、図 2 に示すように、テレビ受像機 8 2 の前面枠部分 8 1 に、無線 IC タグ 8 0 a を貼り付け、貼り付けた無線 IC タグ 8 0 a の上面に、ロゴマーク 8 3 を貼り付ける。また、衣服の生産業者は、図 3 に示すように、ラベル 9 3 の裏面に無線 IC タグ 8 0 b を貼り付け、無線 IC タグ 8 0 b を貼り付けたラベル 9 3 を衣服 9 0 の襟裏側部 9 1 に縫い付ける。

## 【0016】

無線ＩＣタグは、前記製品に関する情報を記憶する領域を備えている。生産業者は、生産の工程において、無線ＩＣタグに生産に関する情報を書き込み、又は無線ＩＣタグから参照することにより、製品の生産管理を行う。物流業者は、製品の輸送の過程において、無線ＩＣタグに輸送に関する情報を書き込み、又は無線ＩＣタグから参照することにより、製品の輸送管理を行う。同様に、販売業者、サービス業者及び回収リサイクル業者は、それぞれの業務のプロセスにおいて、無線ＩＣタグにそれぞれの業務に関する情報を書き込み、又は無線ＩＣタグから参照することにより、製品の業務管理を行う。

## 【0017】

このように、複数のステージにおいて、製品に付された１個の無線ＩＣタグに対して、情報の書込みと参照とが行われる。

## 1. 2 ライフサイクル管理システム１０の構成

ライフサイクル管理システム１０は、図４に示すように、生産管理サブシステム２０a、物流管理サブシステム２０b、販売管理サブシステム２０c、サービス管理サブシステム２０d、回収リサイクル管理サブシステム２０e及びインターネット３０から構成されている。各サブシステムは、インターネット３０を介して相互に接続されている。

## 【0018】

生産管理サブシステム２０a、物流管理サブシステム２０b、販売管理サブシステム２０c、サービス管理サブシステム２０d及び回収リサイクル管理サブシステム２０eは、それぞれ、前記生産業者、前記物流業者、前記販売業者、前記サービス業者及び前記回収リサイクル業者による製品の管理を行うための情報管理システムである。

## 1. 3 サブシステム２０の構成

生産管理サブシステム２０a、物流管理サブシステム２０b、販売管理サブシステム２０c、サービス管理サブシステム２０d及び回収リサイクル管理サブシステム２０eは、共通の構成を有している。これらのサブシステムをサブシステム２０として、以下において説明する。

## (1) サブシステム20の構成

サブシステム20は、図5に示すように、物品に貼り付けられた無線ICタグ80とリーダライタ30a(30b)と管理装置40a(40b)とからなる第1組、携帯電話型リーダライタ30cと基地局50と受信装置51と接続装置53とからなる第2組、リーダライタ30dと携帯電話内蔵型管理装置40dと基地局50と受信装置51と接続装置53とからなる第3組、携帯端末型リーダライタ30eとICカード52と管理装置40eとからなる第4組、データベース61を有するホストコンピュータ60及びLAN装置70から構成される。

## 【0019】

第1組において、リーダライタ30a(30b)は管理装置40a(40b)に接続され、管理装置40a(40b)はLAN装置70に接続されている。

第2組において、携帯電話型リーダライタ30cは、基地局50及び公衆回線網を介して、受信装置51と通信を行い、受信装置51は接続装置53に接続され、接続装置53はLAN装置70に接続されている。

## 【0020】

第3組において、リーダライタ30dは、携帯電話内蔵型管理装置40dに接続され、携帯電話内蔵型管理装置40dは、基地局50及び公衆回線網を介して、受信装置51と通信を行い、受信装置51は接続装置53に接続され、接続装置53はLAN装置70に接続されている。

第4組において、ICカード52は携帯端末型リーダライタ30e又は管理装置40eに装着される。携帯端末型リーダライタ30eはICカード52にデータを書込み、又はICカード52からデータを参照する。また、管理装置40eはICカード52にデータを書込み、又はICカード52からデータを参照する。管理装置40eは、LAN装置70に接続されている。

## 【0021】

ホストコンピュータ60は、LAN装置70に接続されている。

また、LAN装置70は、インターネット30に接続されている。

## (2) 第1組のリーダライタ30a及び管理装置40a

生産管理サブシステム20aに含まれる第1組のリーダライタ30a及び管理



装置40aが、生産工場内に設置されている状況を、図6に示す。この図に示すように、生産工場内において、無線ICタグが張り付けられたテレビ受像機が段ボール箱内に梱包され、テレビ受像機の梱包された段ボール箱がベルトコンベア上を移動している。この図に示すように、管理装置40aは、所謂パーソナルコンピュータと同様に、ディスプレイ部と本体部とキーボード部とから構成されている。また、リーダライタ30aは、円筒形状を有する本体部と本体部上端に備えられたアンテナ部から構成され、アンテナ部と、リーダライタ30aの近辺のベルトコンベア上を移動する段ボール箱との間において、アンテナ部から送信される電波を遮る物がないように、ベルトコンベアに近接して設置されている。

(3) 第3組のリーダライタ30d及び携帯電話内蔵型管理装置40d

物流管理サブシステム20bに含まれる第3組のリーダライタ30d及び携帯電話内蔵型管理装置40dが、貨物トラックに搭載されている様子を、図7に示す。この図に示すように、携帯電話内蔵型管理装置40dは、所謂ノートブック型パーソナルコンピュータと同様に、液晶ディスプレイ部とキーボードを兼ねた本体部と基地局50と間で電波の送受信を行うアンテナ部とから構成され、貨物トラックの助手席前方に設置されている。また、リーダライタ30dは、アンテナ部を有し、貨物トラックの荷物搬入口の上部内側において、アンテナ部から下向に電波が送信されるように、取り付けられている。

(4) 第2組の携帯電話型リーダライタ30c

物流管理サブシステム20bに含まれる第2組の携帯電話型リーダライタ30cの外観を図8に示す。携帯電話型リーダライタ30cは、所謂携帯電話と同様の形状を有する本体部からなり、本体部の前端側面において、基地局50と間で電波の送受信を行い、無線ICタグとの間で電波を送受信するアンテナ部とを備え、本体部の操作側面において、複数の操作ボタンと表示部とマイクとスピーカとを備えている。

(5) 第1組のリーダライタ30b

販売管理サブシステム20cに含まれる第1組のリーダライタ30bの外観を図9に示す。リーダライタ30bは、円筒形状の本体部を有し、本体部の前端側面に無線ICタグとの間で電波を送受信するアンテナ部を備え、本体部側面に操

作ボタンを備えている。第 1 組のリーダライタ 3 0 b は、同一時間帯において、複数の無線 I C タグとの間でデータの読み書きを行う。

#### (6) 第 4 組の携帯端末型リーダライタ 3 0 e

サービス管理サブシステム 2 0 d に含まれる第 4 組の携帯端末型リーダライタ 3 0 e の外観を図 1 0 に示す。携帯端末型リーダライタ 3 0 e は、本体部の前端側面において、無線 I C タグとの間で電波を送受信するアンテナ部とプリンタ部とを備え、本体部側面において、複数の操作ボタンと表示部とを備え、本体部の後端側面において、I C カード挿入口を備えており、I C カード挿入口には、I C カード 5 2 が装着される。また、管理装置 4 0 e は、所謂パーソナルコンピュータと同様に、ディスプレイ部と本体部とキーボード部とを含み、さらに I C カード入出力部を備えており、I C カード入出力部には、I C カード 5 2 が装着される。

#### 1. 4 リーダライタ 3 0 の構成

リーダライタ 3 0 a、3 0 b 及び 3 0 d は、同様の構成を有する。また、携帯電話型リーダライタ 3 0 c、携帯端末型リーダライタ 3 0 e は、リーダライタ 3 0 a と同様の構成を内蔵する。ここでは、これらの装置をリーダライタ 3 0 として説明する。

#### 【 0 0 2 2 】

リーダライタ 3 0 は、同一時間帯において、最大 5 0 個の無線 I C タグに対して情報の読み書きができる。リーダライタ 3 0 は、図 1 1 に示すように、入出力部 1 0 1、制御部 1 0 2、一時記憶部 1 0 3、命令生成部 1 0 4、クロック生成部 1 0 5、識別コード記憶部 1 0 6、鍵記憶部 1 0 7、暗号化部 1 0 8、ハッシュ部 1 0 9、命令解説部 1 1 0、変復調部 1 1 1 及びアンテナ部 1 1 2 から構成される。

#### (1) 一時記憶部 1 0 3

一時記憶部 1 0 3 は、無線 I C タグを識別する 5 0 個の識別コードをそれぞれ一時的に記憶する 5 0 個の識別コード領域を有する。

#### (2) 識別コード記憶部 1 0 6

識別コード記憶部 1 0 6 は、それぞれ 5 0 個の識別コードを記憶する領域を有

する。

### (3) 鍵記憶部 107

鍵記憶部 107 は、リーダライタ 30 に許可されている無線 IC タグの後述するステージ領域の 1 個をアクセスするための領域鍵 K1 と、無線 IC タグの後述する共通領域をアクセスするための領域鍵 K6 とを記憶している。これらの領域鍵は、56 ビット長である。

#### 【0023】

なお、リーダライタ 30 に許可されている無線 IC タグのステージ領域が、前記 1 個のステージ領域以外のステージ領域である場合には、そのステージ領域に応じて、領域鍵 K1 の代わりに、領域鍵 K2～K5 のいずれか 1 個を記憶している。領域鍵 K2～K5 は、それぞれ 56 ビット長である。

### (4) 入出力部 101

入出力部 101 は、後述する管理装置 40 と接続されており、管理装置 40 から入出力命令と入出力情報とからなる組を受け取る。

#### 【0024】

入出力命令は、入力命令又は出力命令からなる。入力命令は、無線 IC タグが有するメモリからデータを読み出す命令であり、出力命令は、無線 IC タグが有するメモリにデータを書き込む命令である。入出力命令が入力命令である場合に、入出力情報は、無線 IC タグのメモリの物理アドレスと読み出しバイト数とを含む。入出力命令が出力命令である場合に、入出力情報は、無線 IC タグのメモリの物理アドレスと書込みバイト数と書込み内容とを含む。

#### 【0025】

入出力部 101 は、受け取った入出力命令と入出力情報とを制御部 102 へ出力する。また、制御部 102 からアクセス応答命令とアクセス応答情報と識別コードとを受け取り、管理装置 40 へ受け取ったアクセス応答命令とアクセス応答情報と識別コードとを出力する。

### (5) 制御部 102

制御部 102 は、図 12 に示すように、充電電波送信期間、同期信号送信期間、識別コード収集期間及びアクセス期間において、それぞれ、充電電波送信の制

御、同期信号送信の制御、識別コード収集の制御及びアクセスの制御を行う。この図において、横軸は時間軸である。

#### 【0026】

充電電波送信期間、同期信号送信期間、識別コード収集期間及びアクセス期間は、この順序で時間軸上で隣接している。

識別コード収集期間は、第1収集期間と第2収集期間とからなり、第1収集期間と第2収集期間とは、それぞれ、識別コード送信期間、識別コード応答期間及び識別コード一致期間から構成される。識別コード送信期間、識別コード応答期間及び識別コード一致期間は、それぞれ、500m秒長の一周期を形成する。

#### 【0027】

1周期は、50個の10m秒長に均等に分割される。各10m秒長を、チャンネルと呼ぶ。1周期内の50個のチャンネルを、1周期の先頭から順にそれぞれチャンネル1、チャンネル2、チャンネル3、・・・チャンネル50と呼び、50個のチャンネルは、これらのチャンネル番号により識別される。

#### (命令の出力)

制御部102は、入出力部101から、入出力命令と入出力情報とを受け取る。入出力命令を受け取ると、命令生成部104に対して、同期信号を送信する旨の同期信号送信命令及び各無線ICタグの識別コードを収集する旨の識別コード収集命令をこの順序で出力する。

#### (識別コードの収集)

制御部102は、命令生成部104に対して、識別コード収集命令を出力した後、3秒間の識別コード収集期間において、次に示すようにして、各無線ICタグから識別コードを収集する。前記識別コード収集期間が経過すると、制御部102は、各無線ICタグから識別コードの収集が終了したとみなし、識別コードの収集を終了する。識別コード収集期間は、上記に説明したように、第1収集期間と第2収集期間とに分かれており、第1収集期間と第2収集期間とのそれぞれにおいて、制御部102は、識別コード送信の制御、識別コード応答の制御、識別コード一致の制御を行う。このように、第1収集期間と第2収集期間とのそれぞれにおいて、2回の収集を行う理由については、後述する。

## 【 0 0 2 8 】

制御部 1 0 2 は、識別コード送信期間において、命令解読部 1 1 0 から識別コード送信命令と識別コードとを受け取り、ハッシュ部 1 0 9 からハッシュ値を受け取る。識別コード送信命令を受け取ると、受け取った識別コードを、一時記憶部 1 0 3 内の前記受け取ったハッシュ値により示される識別コード領域へ書き込む。

## 【 0 0 2 9 】

制御部 1 0 2 は、クロック生成部 1 0 5 から基準クロックを受け取り、受け取った基準クロックに基づいて、1 0 m 秒間に 1 個のパルス信号からなる同期信号を繰り返し含む同期信号波を生成し、生成した同期信号波を 1 0 0 m 秒間、命令生成部 1 0 4 へ出力する。

図 1 2 に示すように、同期信号波の 1 周期は、5 0 0 m 秒であり、前述したように、1 周期は、5 0 個の 1 0 m 秒長に均等に分割され、各 1 0 m 秒長を、チャンネルと呼ぶ。

## 【 0 0 3 0 】

制御部 1 0 2 は、受け取ったハッシュ値をチャンネル番号とするチャンネルを選択し、識別コード応答期間内の、選択したチャンネルにおいて、前記受け取った識別コードと、前記識別コードを送信する旨を示す識別コード応答命令とを命令生成部 1 0 4 へ出力する。

このように、制御部 1 0 2 は、受け取ったハッシュ値をチャンネル番号としてチャンネルを選択するので、異なる無線 I C タグに対して同じチャンネルが選択される可能性がある。この場合において、これらの無線 I C タグについては、第 1 収集期間における識別コードの収集は諦め、第 2 収集期間において、これらの無線 I C タグの識別コードの収集を行う。この第 2 収集期間において、これらの異なる無線 I C タグに対して同じチャンネルが選択される可能性は低くなる。

## 【 0 0 3 1 】

制御部 1 0 2 は、識別コード一致期間内の選択したチャンネルにおいて、命令解読部 1 1 0 から識別コード一致命令の受け取りを待ち受ける。選択したチャンネルにおいて、命令解読部 1 1 0 から識別コード一致命令を受け取ると、前記一時記

憶部 1 0 3 の前記ハッシュ値により示される識別コード領域に記憶されている識別コードが正しく前記無線 I C タグを識別する識別コードであると認識し、前記一時記憶部 1 0 3 に記憶されている前記識別コード読み出し、読み出した識別コードを識別コード記憶部 1 0 6 へ書き込む。

(無線 I C タグからの認証と領域アクセス)

制御部 1 0 2 は、識別コード記憶部 1 0 6 に記憶されている全ての識別コードについて、以下に示すように、アクセス期間において、各識別コードにより識別される無線 I C タグへのアクセス要求と無線 I C タグの領域アクセスとを行う。

【 0 0 3 2 】

制御部 1 0 2 は、アクセス期間において、識別コード記憶部 1 0 6 から 1 個の識別コードを読み出し、読み出した識別コードにより識別される無線 I C タグに対するアクセスを要求する旨のアクセス要求命令と、前記読み出した識別コードとを命令生成部 1 0 4 へ出力する。

制御部 1 0 2 は、命令解読部 1 1 0 から認証子送信命令と識別コードとを受け取る。認証子送信命令を受け取ると、鍵記憶部 1 0 7 に記憶されている領域鍵 ( K 1 又は K 6 ) を読み出し、読み出した領域鍵 ( K 1 又は K 6 ) を暗号化部 1 0 8 へ出力する。読み出す領域鍵が K 1 であるか又は K 6 であるかは、入出力部 1 0 1 から受け取る入出力情報により決定する。入出力情報に含まれる物理アドレスが、リーダライタ 3 0 に許可されている無線 I C タグのステージ領域内を示す場合には、K 1 を読み出す。入出力情報に含まれる物理アドレスが、リーダライタ 3 0 の共通領域内を示す場合には、K 6 を読み出す。

【 0 0 3 3 】

制御部 1 0 2 は、命令生成部 1 0 4 へ前記読み出した識別コードと認証子応答命令とを出力する。

制御部 1 0 2 は、命令解読部 1 1 0 からアクセス不許可命令と識別コードと理由コードとを受け取る。アクセス不許可命令と識別コードと理由コードとを受け取ると、受け取った理由コードに基づいて、領域鍵 K 1 の誤り等操作の誤りであると認識し、識別コードで識別される無線 I C タグへのアクセスを諦める。次にアクセス応答命令を生成し、理由コードを含むアクセス応答情報を生成し、アク

セス応答命令とアクセス応答情報と識別コードとを入出力部101へ出力する。

【0034】

制御部102は、入出力命令に基づいてアクセス命令を生成し、入出力情報に基づいてアクセス情報を生成し、命令生成部104へ、前記読み出した識別コードとアクセス情報とアクセス命令とを出力する。

制御部102は、命令解読部110から、アクセス応答命令とアクセス応答情報と識別コードとを受け取り、受け取ったアクセス応答命令とアクセス応答情報と識別コードとを入出力部101へ出力する。

【0035】

なお、各命令は、4ビット長からなるコードである。

制御部102は、無線ICタグから放射される電波を受信する期間内において、変復調部111に対して、無信号波を出力するように、制御する。この期間とは、識別コード送信期間、識別コード一致期間、アクセス期間であり、無線ICタグからデータを受信する期間である。

(6) 命令生成部104

命令生成部104は、制御部102から、同期信号送信命令、識別コード収集命令、識別コードと識別コード応答命令との組、アクセス要求命令と識別コードとの組、識別コードと認証子応答命令との組、及び識別コードとアクセス情報とアクセス命令との組を受け取る。

【0036】

これらの命令と命令に付随するオペランド等を図13に示す。

命令生成部104は、制御部102から同期信号送信命令を受け取ると、受け取った同期信号送信命令に基づいて、パルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。続いて、制御部102から同期信号波を受け取り、受け取った同期信号波に基づいて、パルス信号波を1秒間生成し、生成したパルス信号波を変復調部111へ出力する。

【0037】

命令生成部104は、制御部102から識別コード収集命令、識別コード応答命令、アクセス要求命令、認証子応答命令又はアクセス命令を受け取ると、それ

ぞれの命令に基づいて、パルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。

命令生成部104は、制御部102から識別コードと識別コード応答命令とを受け取ると、識別コード応答命令に基づくパルス信号波の出力に引き続いて、受け取った識別コードに基づいてパルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。

#### 【0038】

命令生成部104は、制御部102からアクセス要求命令と識別コードとを受け取ると、アクセス要求命令に基づくパルス信号波の出力に引き続いて、受け取った識別コードに基づいてパルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。

命令生成部104は、制御部102から識別コードと認証子応答命令とを受け取り、暗号化部108から暗号化乱数R0'を受け取ると、認証子応答命令に基づくパルス信号波の出力に引き続いて、受け取った識別コードと暗号化乱数R0'とに基づいてパルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。

#### 【0039】

命令生成部104は、制御部102から識別コードとアクセス情報とアクセス命令とを受け取ると、アクセス命令に基づくパルス信号波の出力に引き続いて、受け取った識別コードとアクセス情報とに基づいてパルス信号波を生成し、生成したパルス信号波を変復調部111へ出力する。

#### (7) クロック生成部105

クロック生成部105は、基準時刻を示す基準クロックを繰り返し生成し、生成した基準クロックを制御部102へ出力する。

#### (8) 暗号化部108

暗号化部108は、暗号アルゴリズムE1を備えている。ここで、暗号アルゴリズムE1は、DES（データ暗号化規格、Data Encryption Standard）により規定されている暗号アルゴリズムである。この暗号アルゴリズムの暗号鍵は56ビット長であり、この暗号アルゴリズムE1に入力さ



れる平文及びこの暗号アルゴリズムE 1により生成される暗号文の長さは64ビットである。

#### 【0040】

暗号化部108は、制御部102から領域鍵(K 1又はK 6)を受け取り、命令解読部110から乱数R 0を受け取り、領域鍵(K 1又はK 6)を用いて、受け取った乱数R 0に暗号アルゴリズムE 1を施して、暗号化乱数R 0'を生成し、生成した暗号化乱数R 0'を命令生成部104へ出力する。

なお、この明細書において、鍵Kを用いて、平文Mに対して、暗号アルゴリズムEを施し、暗号文Cを生成するとき、次の式に示すように表現することとする。

#### 【0041】

$$C = E(M, K)$$

#### (9) ハッシュ部109

ハッシュ部109は、命令解読部110から乱数R 0を受け取り、受け取った乱数R 0を入力値として、ハッシュ関数Hを施して、ハッシュ値を生成する。

生成されるハッシュ値は、1～50の50個の値のうちのいずれかの1個の値をとる。前記ハッシュ関数Hは、入力値に基づいて、入力値を前記50個の値に均等に振り分け、入力値が振り分けられた1個の値をハッシュ値として生成する。

#### 【0042】

ハッシュ部109は、生成したハッシュ値を制御部102へ出力する。

#### (10) 命令解読部110

命令解読部110は、変復調部111からパルス信号波を受け取る。受け取ったパルス信号波を解読して、命令とオペランドとを抽出し、抽出した命令を制御部102へ出力する。抽出する命令には、図14に示すように、識別コード送信命令、識別コード一致命令、認証子送信命令、アクセス不許可命令及びアクセス応答命令が含まれる。これらの命令は、4ビット長からなる命令である。

#### 【0043】

命令解読部110は、抽出した命令が識別コード送信命令である場合に、オペ

ランドとして、乱数R0と識別コードとを抽出し、抽出した乱数R0をハッシュ部109へ出力し、抽出した識別コードを制御部102へ出力する。

命令解読部110は、抽出した命令が認証子送信命令である場合に、オペランドとして、乱数R0と識別コードとを抽出する。ここで、乱数R0は、リーダーのステージ領域を認証するための認証子である。抽出した乱数R0を暗号化部108へ出力し、抽出した識別コードを制御部102へ出力する。

#### 【0044】

命令解読部110は、抽出した命令が識別コード一致命令である場合に、オペランドとして、識別コードを抽出し、抽出した識別コードを制御部102へ出力する。

命令解読部110は、抽出した命令がアクセス不許可命令である場合に、オペランドとして、識別コードと理由コードとを抽出し、抽出した識別コードと理由コードとを制御部102へ出力する。

#### 【0045】

命令解読部110は、抽出した命令がアクセス応答命令である場合に、オペランドとして、アクセス応答情報と識別コードとを抽出し、抽出したアクセス応答情報と識別コードとを制御部102へ出力する。

#### (11) 変復調部111

変復調部111は、命令生成部104からパルス信号波又は無信号波を受け取る。また、制御部102から無信号波を受け取る。パルス信号波を受け取ると、受け取ったパルス信号波を変調信号として、変調信号に基づいて2.45GHzの搬送波の振幅を変化させ、振幅の変化した搬送波をアンテナ部112へ出力する。また、無信号波を受け取ると、2.45GHzの搬送波をそのまま、アンテナ部112へ出力する。

#### 【0046】

また、変復調部111は、アンテナ部112から電力信号を受け取り、受け取った電力信号から2.45GHzの周波数を有する信号を選択し、選択した信号からパルス信号波を抽出し、抽出したパルス信号波を命令解読部110へ出力する。

## (12) アンテナ部 112

アンテナ部 112 は、送信アンテナと受信アンテナとから構成される。

## 【0047】

アンテナ部 112 は、送信アンテナとして、特定の方向に電波を放射する指向性アンテナである。変復調部 111 から振幅の変化した、又は変化していない搬送波を受け取り、電波として空間に放射する。

アンテナ部 112 は、受信アンテナとして、電波を受信し、受信した電波を電力信号に変換して、電力信号を変復調部 111 へ出力する。

## 1.5 無線 IC タグ 80 の構成

無線 IC タグ 80 は、図 15 に示すように、長さ 30 mm、幅 5 mm、厚さ 0.5 mm の板状に成形された樹脂内に、IC チップ部 200 とアンテナ部 201 とが、封入されて形成されている。

## 【0048】

なお、無線 IC タグの形成方法については、特開平 8-276458 号公報に記載されているので、詳細の説明を省略する。

無線 IC タグ 80 の通信可能な距離は、1 m 程度以内であり、通信速度は、10~20 m 秒 / byte である。また、無線 IC タグ 80 は、50 枚以内の重ね読み（マルチ読み）が可能である。

## 【0049】

IC チップ部 200 は、図 16 に示すように、電源部 203、復調部 206、命令解読部 207、識別コード記憶部 208、制御部 209、認証部 210、乱数生成部 211、ハッシュ部 212、変調部 213、クロック生成部 214、入出力部 215 及びメモリ部 216 から構成される。

IC チップ部 200 の寸法は、縦 1 mm、横 1 mm、厚さ 0.25 ミクロンである。

## (1) 識別コード記憶部 208

識別コード記憶部 208 は、無線 IC タグ 80 を個別に識別する識別コードを記憶している。識別コードは、32 ビットからなり、無線 IC タグを製造する製造業者を識別する製造業者識別コード（10 ビット長）と、無線 IC タグが複数

の仕様や種類を有する場合に、その仕様や種類などを識別する種類コード（10ビット長）と、製造業者及び種類毎に個別に異なる値が設定される製造番号（12ビット長）とから構成される。

## （2）メモリ部 2 1 6

メモリ部 2 1 6 は、1 K バイトの記憶容量を有する E E p r o m ( E l e c t r o n i c E r a s a b l e a n d P r o g r a m m a b l e R O M ) から構成される。

### 【 0 0 5 0 】

なお、E E p r o m に代えて、ヒューズ R O M を用いるとしてもよい。ヒューズ R O M は、一度データを書き込むと消去することができないタイプのメモリである。ヒューズ R O M を用いることにより、データの改竄を防ぐことができる。また、E E p r o m 及びヒューズ R O M の両方を用いるとしてもよい。

メモリ部 2 1 6 は、図 1 7 に示すように、非プロテクト部 3 0 1 とプロテクト部 3 0 2 とから構成され、非プロテクト部 3 0 1 は、アドレス 0 ～ 2 4 9 （10進数表示。以下同様にアドレスは10進数表示。）に配置され、250 バイトからなり、プロテクト部 3 0 2 は、アドレス 2 5 0 ～ 9 9 9 に配置され、750 バイトからなる。

### 【 0 0 5 1 】

非プロテクト部 3 0 1 は、50 バイトずつ5個の領域 3 1 1 ～ 3 1 5 から構成され、領域 3 1 1 ～ 3 1 5 は、それぞれ、アドレス 0 ～ 4 9、50 ～ 9 9、100 ～ 1 4 9、150 ～ 1 9 9、200 ～ 2 4 9 に配置されている。プロテクト部 3 0 2 は、150 バイトずつ5個の領域 3 2 1 ～ 3 2 5 から構成され、領域 3 2 1 ～ 3 2 5 は、それぞれ、アドレス 2 5 0 ～ 3 9 9、400 ～ 5 4 9、550 ～ 6 9 9、700 ～ 8 4 9、850 ～ 9 9 9 に配置されている。

### 【 0 0 5 2 】

領域 3 1 1 及び領域 3 2 1、領域 3 1 2 及び領域 3 2 2、領域 3 1 3 及び領域 3 2 3、領域 3 1 4 及び領域 3 2 4、領域 3 1 5 及び領域 3 2 5 は、それぞれ、5 個の生産ステージ、物流ステージ、販売ステージ、サービスステージ、回収リサイクルステージのために用いられるステージ領域である。

領域 3 1 1 ～ 3 1 5 は、領域鍵 K 6 によるアクセスが許可される共通領域である。領域 3 2 1 ～ 3 2 5 は、それぞれ領域鍵 K 1 ～ K 5 のみによるアクセスが許可される領域である。

#### 【 0 0 5 3 】

ここで、領域鍵 K 6 によりこれらの共通領域へのアクセスが許可されるとしているのは、領域鍵 K 6 を知る者へのみアクセスを許可することにより、不用意にデータの読み書きがされないようにするためである。

領域 3 2 1 ～ 3 2 5 は、それぞれ 1 度だけ書込みを行うライトワンス (Write Once) 部と更新が可能な可変部とからなる。

#### 【 0 0 5 4 】

各領域に情報が記録されているメモリ部 2 1 6 の一例を図 1 8 に示す。この図において、メモリ部 2 1 6 の内容をステージ領域毎に示している。

生産ステージ領域には、非プロテクト部において、「メーカー名」、「品名」及び「品番」が記録され、プロテクト部のライトワンス部において、「製番」、「製造日」及び「工場名」が記録されている。

#### 【 0 0 5 5 】

物流ステージ領域には、非プロテクト部において、「運送業者名」が記録され、プロテクト部のライトワンス部において、「入出庫日」及び「グローバルロケーション番号 (GLN)」が記録されている。

販売ステージ領域には、非プロテクト部において、「保証期間」及び「保証番号」が記録され、プロテクト部のライトワンス部において、「卸業者名」、「小売店名」及び「販売日」が記録されている。

#### 【 0 0 5 6 】

サービスステージ領域には、非プロテクト部において、「洗濯方法」が記録され、プロテクト部の可変部において、「修理者名」、「修理日」及び「修理部品」が記録されている。

回収リサイクルステージ領域には、プロテクト部のライトワンス部において、「回収業者名」、「回収日」、「廃棄業者」及び「廃棄日」が記録され、プロテクト部の可変部において、「リユース記録」が記録されている。

### (3) 電源部 2 0 3

電源部 2 0 3 は、アンテナ部 2 0 1 と接続され、アンテナ部 2 0 1 から電力信号を受け取り、受け取った電力信号を電荷として蓄積する。また、無線 IC タグ 8 0 の各構成部に電力を供給する。

#### 【 0 0 5 7 】

電源部 2 0 3 に含まれる電源回路の一例を、        に示す。図 1 9 に示す電源回路は、4 個のダイオード D 1 ~ D 4 と、電池 E とから構成される。ダイオード D 1 ~ D 2 は、同じ方向に直列に接続され、ダイオード D 3 ~ D 4 は、同じ方向に直列に接続され、また、ダイオード D 1 ~ D 2 とダイオード D 3 ~ D 4 とは、同じ方向に並列に接続されている。アンテナ部 2 0 1 の一端は、ダイオード D 1 と D 2 との中間点に接続され、アンテナ部 2 0 1 の他の一端は、ダイオード D 3 と D 4 との中間点に接続されている。電池 E の一端は、ダイオード D 1 と D 3 との中間点に接続され、電池 E の他の一端はダイオード D 2 と D 4 との中間点に接続されている。

### (4) 復調部 2 0 6

復調部 2 0 6 は、インピーダンス切換部 2 0 5 から電力信号を受け取り、受け取った電力信号から 2 . 4 5 G H z の周波数を有する信号を選択し、選択した信号からパルス信号波を抽出し、抽出したパルス信号波を命令解読部 2 0 7 へ出力する。

### (5) 命令解読部 2 0 7

命令解読部 2 0 7 は、復調部 2 0 6 からパルス信号波を受け取る。受け取ったパルス信号波を解読して、命令とオペランドとを抽出し、抽出した命令とオペランドとを制御部 2 0 9 へ出力する。抽出する命令には、図 1 3 に示すように、同期信号送信命令、識別コード収集命令、アクセス要求命令、アクセス命令、識別コード応答命令及び認証子応答命令が含まれる。なお、これらの命令及びオペランドについては、前述したとおりであるので、説明は省略する。

### (6) 制御部 2 0 9

制御部 2 0 9 は、命令解読部 2 0 7 から命令とオペランドとを受け取る。これらの命令には、同期信号送信命令、識別コード収集命令、アクセス要求命令、ア

クセス命令、識別コード応答命令及び認証子応答命令が含まれる。また、比較器 235 から、ステージ領域を識別する番号  $X_i$  (後述する) 又は暗号化乱数が一致しない旨を受け取る。

#### 【0058】

制御部 209 は、同期信号送信命令を受け取ると、引き続き復調部 206 から同期信号波を受信し、受信した同期信号波に含まれる同期信号を抽出し、クロック生成部 214 から基準クロックを受け取り、受け取った基準クロックに基づいて、抽出した同期信号に同期する同期信号を繰り返し含む同期信号波を生成する。

#### (識別コードの出力)

制御部 209 は、識別コード収集命令を受け取ると、乱数生成部 211 に対して乱数を生成するように指示する。次に、乱数生成部 211 から生成された乱数  $R_0$  を受け取り、ハッシュ部 212 から生成されたハッシュ値を受け取り、識別コード記憶部から識別コードを読み出す。次に、制御部 209 は、受け取ったハッシュ値をチャンネル番号とするチャンネルを選択し、識別コード送信期間において、選択したチャンネルにより、読み出した識別コードと乱数  $R_0$  と識別コード送信命令とを変調部 213 へ出力する。

#### 【0059】

制御部 209 は、識別コード応答期間において、選択したチャンネルにより、識別コード応答命令を受け取ると、さらに識別コードを受け取り、前記識別コード記憶部 208 から読み出した識別コードと、受け取った識別コードとを比較する。一致しているなら、識別コード一致期間において、選択したチャンネルにより、識別コードと識別コード一致命令とを変調部 213 へ出力する。一致していないなら、上記の乱数生成部 211 に対する乱数生成から再度繰り返す。

#### (アクセスの認証)

制御部 209 は、アクセス期間において、アクセス要求命令を受け取ると、さらに識別コードを受け取る。次に、受け取った識別コードと識別コード記憶部 208 から読み出した識別コードとを比較する。一致しなければ、さらに、アクセス要求命令の受け取りを待ち受ける。一致すれば、乱数生成部 211 に対して乱

数を生成するように指示し、乱数生成部 2 1 1 から乱数 R 0 を受け取り、識別コードと乱数 R 0 と認証子送信命令とを変調部 2 1 3 へ出力する。

## 【 0 0 6 0 】

制御部 2 0 9 は、認証子応答命令を受け取ると、さらに、識別コードと暗号化乱数 R 0 ' を受け取る。次に、受け取った識別コードと識別コード記憶部 2 0 8 から読み出した識別コードとを比較する。一致しなければ、さらに、認証子応答命令の受け取りを待ち受ける。一致すれば、暗号化乱数 R 0 ' を認証部 2 1 0 の比較器 2 3 5 へ出力する。

## 【 0 0 6 1 】

制御部 2 0 9 は、比較器 2 3 5 から暗号化乱数が一致しない旨を受け取ると、識別コードとアクセス不許可命令と理由コードとを変調部 2 1 3 へ出力する。ここで、理由コードは、許可されていないステージ領域のアクセスであることを示す。また、番号 X i を受け取ると、次にアクセス命令を受け取る。

制御部 2 0 9 は、アクセス命令を受け取ると、さらに、識別コードとアクセス情報とを受け取る。アクセス命令は、R e a d 命令及び W r i t e 命令からなる。アクセス命令が R e a d 命令である場合には、アクセス情報は、物理アドレスと読み出しバイト数とを含み、アクセス命令が W r i t e 命令である場合には、アクセス情報は、物理アドレスと書込みバイト数と書込み内容とを含む。次に、受け取った識別コードと識別コード記憶部 2 0 8 から読み出した識別コードとを比較する。

## 【 0 0 6 2 】

一致しなければ、さらに、アクセス命令の受け取りを待ち受ける。一致すれば、アクセス情報に含まれる物理アドレスが番号 X i で示されるステージ領域内を示しているか否かを判断し、ステージ領域内を示していない場合には、識別コードとアクセス不許可命令と理由コードとを変調部 2 1 3 へ出力する。ここで、理由コードは、許可されていないステージ領域のアクセスであることを示す。ステージ領域内を示している場合には、受け取ったアクセス命令とアクセス情報とを入出力部 2 1 5 へ出力する。

## 【 0 0 6 3 】



制御部 2 0 9 は、入出力部 2 1 5 から、メモリ部 2 1 6 から読み出した情報又は書込み終了の情報を受け取る。前記読み出した情報又は書込み終了の情報を受け取ると、識別コードとアクセス応答命令とアクセス応答情報とを変調部 2 1 3 へ出力する。ここで、アクセス応答情報は、メモリ部 2 1 6 から読み出した情報又は書込み終了の情報である。

#### (7) 認証部 2 1 0

認証部 2 1 0 は、図 2 0 に示すように、鍵記憶部 2 3 1 と乱数記憶部 2 3 2 と暗号化部 2 3 3 と生成乱数記憶部 2 3 4 と比較器 2 3 5 とを備えている。

##### (a) 鍵記憶部 2 3 1

鍵記憶部 2 3 1 は、無線 IC タグ 8 0 の 5 個のステージ領域をそれぞれアクセスするための領域鍵 K 1 ~ K 5 と、共通領域をアクセスするための領域鍵 K 6 とを記憶している。これらの領域鍵は、それぞれ 5 6 ビット長である。

##### (b) 乱数記憶部 2 3 2

乱数記憶部 2 3 2 は、乱数生成部 2 1 1 から乱数 R 0 を受け取り、受け取った乱数 R 0 を記憶する。

##### (c) 暗号化部 2 3 3

暗号化部 2 3 3 は、暗号化部 1 0 8 が備える暗号アルゴリズム E 1 と同じ暗号アルゴリズム E 1 を備えている。

#### 【 0 0 6 4 】

暗号化部 1 0 8 は、鍵記憶部 2 3 1 から領域鍵 K 1 ~ K 6 を読み出し、乱数記憶部 2 3 2 から乱数 R 0 を読み出し、読み出した領域鍵 K 1 ~ K 6 を用いて、読み出した乱数 R 0 に暗号アルゴリズム E 1 を施して、それぞれ暗号化乱数 R 1 ~ R 6 を生成し、生成した暗号化乱数 R 1 ~ R 6 を生成乱数記憶部 2 3 4 に書き込む。

##### (d) 生成乱数記憶部 2 3 4

生成乱数記憶部 2 3 4 は、暗号化乱数 R 1 ~ R 6 を記憶する。

##### (e) 比較器 2 3 5

比較器 2 3 5 は、命令解読部 2 0 7 から暗号化乱数 R 0' を受け取り、受け取った暗号化乱数 R 0' に一致する暗号化乱数を生成乱数記憶部 2 3 4 から捜し、

一致する暗号化乱数があれば、一致する暗号化乱数を識別する番号  $X_i$  を制御部 209 へ出力する。例えば、一致する暗号化乱数が  $R_1$  であれば、番号  $X_i$  は、1 であり、一致する暗号化乱数が  $R_2$  であれば、番号  $X_i$  は、2 である。この番号  $X_i$  は、ステージ領域を識別する番号である。番号  $X_i$  が 1～5 の場合、それぞれ、生産用、物流用、販売用、サービス用、回収リサイクル用のステージ領域を識別する。

【0065】

一致する暗号化乱数がなければ、暗号化乱数が一致しない旨を制御部 209 へ出力する。

#### (8) 乱数生成部 211

乱数生成部 211 は、制御部 209 から乱数生成の指示を受け取る。前記指示を受け取ると、乱数  $R_0$  を生成する。乱数  $R_0$  は、160 ビット長である。生成した乱数  $R_0$  をハッシュ部 212 と認証部 210 と制御部 209 とへ出力する。

#### (9) ハッシュ部 212

ハッシュ部 212 は、乱数生成部 211 から乱数  $R_0$  を受け取り、受け取った乱数  $R_0$  を入力値として、ハッシュ関数  $H$  を施して、ハッシュ値を生成する。

【0066】

ここで、ハッシュ関数  $H$  は、ハッシュ部 109 が有するハッシュ関数と同じ関数である。生成されるハッシュ値は、1～50 の 50 個の値のうちのいずれかの 1 個の値をとる。ハッシュ関数  $H$  は、入力値に基づいて、入力値を前記 50 個の値に均等に振り分け、入力値が振り分けられた 1 個の値をハッシュ値として生成する。

【0067】

ハッシュ部 212 は、生成したハッシュ値を制御部 209 へ出力する。

#### (10) 変調部 213

変調部 213 は、制御部 102 から命令とオペランドとを受け取り、命令とオペランドとからなるビット列を生成し、生成したビット列に含まれるビット (0 又は 1) に応じて、アンテナ部 201 が有するインピーダンスを切り換える。具体的には、各ビットが「1」のとき、前記インピーダンスを第 1 の値とし、各ビ

ットが「0」のとき、第2の値とする。これにより、アンテナ部201から再放射される電波の振幅及び位相を変えることができ、この振幅及び位相の変化により情報を伝達することができる。

#### (11) クロック生成部214

クロック生成部214は、基準時刻を示す基準クロックを繰り返し生成し、生成した基準クロックを制御部209へ出力する。

#### (12) 入出力部215

入出力部215は、制御部209からアクセス命令とアクセス情報とを受け取る。アクセス命令は、Read命令及びWrite命令からなる。アクセス命令がRead命令である場合には、アクセス情報は、物理アドレスと読み出しバイト数とを含み、アクセス命令がWrite命令である場合には、アクセス情報は、物理アドレスと書込みバイト数と書込み内容とを含む。

#### 【0068】

入出力部215は、アクセス命令がRead命令である場合には、メモリ部216の前記物理アドレスにより示される位置から、前記読み出しバイト数分の情報を読み出し、読み出した情報を制御部209へ出力する。

入出力部215は、アクセス命令がWrite命令である場合には、メモリ部216の前記物理アドレスにより示される位置から、前記書込みバイト数分、前記書込み内容を書き込み、書込み終了の情報を制御部209へ出力する。

#### 【0069】

ここで書込み終了の情報とは、書込みが正常に終了したか否かを示し、正常に終了していない場合には、さらに、その理由を示す情報を含む。

#### (13) アンテナ部201

アンテナ部201は、受信アンテナであり、電波を受信し、受信した電波を電力信号に変換して、電力信号を復調部206及び電源部203へ出力する。また、受信した電波を反射（再放射）する。

### 1. 6 管理装置40の構成

管理装置40a及び40bは、同様の構成を有する。また、携帯電話型リーダーライタ30c、携帯電話内蔵型管理装置40d及び携帯端末型リーダーライタ30

e は、管理装置 4 0 a と同様の構成を内蔵する。ここでは、これらの装置を管理装置 4 0 として説明する。

## 【 0 0 7 0 】

管理装置 4 0 は、図 2 1 に示すように、情報記憶部 4 0 1、制御部 4 0 2、LAN 接続部 4 0 3 及び入出力部 4 0 4 から構成され、具体的には、マイクロプロセッサ、ハードディスク、ROM (Read Only Memory)、RAM (Random Access Memory) などから構成される。

## (1) 入出力部 4 0 4

入出力部 4 0 4 は、リーダライタ 3 0 の入出力部 1 0 1 と接続されており、制御部 4 0 2 から入出力命令と入出力情報とからなる組を受け取り、受け取った入出力命令と入出力情報とからなる組を入出力部 1 0 1 へ出力する。

## 【 0 0 7 1 】

また、入出力部 4 0 4 は、入出力部 1 0 1 からアクセス応答命令とアクセス応答情報と識別コードとを受け取り、受け取ったアクセス応答命令とアクセス応答情報と識別コードとを制御部 4 0 2 へ出力する。

## (2) 制御部 4 0 2

制御部 4 0 2 は、入出力命令と入出力情報とからなる組を生成し、生成した入出力命令と入出力情報とからなる組を入出力部 4 0 4 へ出力する。

## 【 0 0 7 2 】

入出力命令は、入力命令又は出力命令からなる。入力命令は、無線 IC タグのメモリからデータを読み出す命令であり、出力命令は、無線 IC タグのメモリにデータを書き込む命令である。入出力命令が入力命令である場合に、入出力情報は、無線 IC タグのメモリの物理アドレスと読み出しバイト数とを含む。入出力命令が出力命令である場合に、入出力情報は、無線 IC タグのメモリの物理アドレスと書込みバイト数と書込み内容とを含む。

## 【 0 0 7 3 】

制御部 4 0 2 は、平文を暗号鍵を用いて暗号化して暗号文を生成する暗号アルゴリズム E 2 と、前記暗号アルゴリズム E 2 により生成された暗号文を復号鍵を用いて解読して平文を生成する復号アルゴリズム B 2 とを有している。ここで、

この暗号アルゴリズム E 2 は、前記暗号アルゴリズム E 1 とは別の暗号アルゴリズムである。なお、同一の暗号アルゴリズムであるとしてもよい。

【0074】

制御部 402 は、入力命令に対応する入力情報を生成する際に、「メーカー名」や「運送業者名」などの入力情報を前記暗号鍵を用いて暗号アルゴリズム E 2 により暗号化して暗号文を生成し、生成した暗号文を入力情報とする。なお、暗号化しないとしてもよい。

また、制御部 402 は、入出力部 404 からアクセス応答命令とアクセス応答情報と識別コードとを受け取り、受け取ったアクセス応答命令が、入力命令に対応する場合に、アクセス応答情報を前記復号鍵を用いて復号アルゴリズム B 2 により復号して平文を生成し、アクセス応答情報としての生成した前記平文と識別コードとを情報記憶部 401 へ書き込む。なお、暗号化されていないアクセス応答情報については、復号しないとしてもよい。

【0075】

また、制御部 402 は、LAN 接続部 403 を介して、ホストコンピュータ 60 から情報を受け取り、受け取った情報を情報記憶部 401 に書き込む。また、情報記憶部 401 に記憶されている情報を、LAN 接続部 403 を介して、ホストコンピュータ 60 へ出力する。

(3) 情報記憶部 401

情報記憶部 401 は、各種の情報を記憶する。

(4) LAN 接続部 403

LAN 接続部 403 は、制御部 402 と LAN 装置 70 とを接続する。

(5) 携帯電話型リーダライタ 30c、携帯電話内蔵型管理装置 40d 及び携帯端末型リーダライタ 30e の構成

携帯電話型リーダライタ 30c、携帯電話内蔵型管理装置 40d 及び携帯端末型リーダライタ 30e は、管理装置 40 と同様の構成を内蔵する。ここでは、管理装置 40 との相違点について簡単に説明する。

【0076】

携帯電話型リーダライタ 30c 及び携帯電話内蔵型管理装置 40d は、LAN

接続部403を備える代わりに、携帯電話機能を有し、携帯電話機能により、基地局50、公衆回線網、受信装置51、接続装置53及びLAN装置70を介して、ホストコンピュータ60と接続される。

また、携帯端末型リーダライタ30eは、LAN接続部403を備える代わりに、ICカード52が装着され、ICカード52により、管理装置40e及びLAN装置70を介して、ホストコンピュータ60と接続される。

#### 1. 7 ホストコンピュータ60の構成

ホストコンピュータ60は、図21に示すように、制御部601、LAN接続部602、DB更新部603及びデータベース61から構成されている。具体的には、マイクロプロセッサ、ハードディスク、ROM (Read Only Memory)、RAM (Random Access Memory) などから構成される。

##### (1) データベース61

データベース61は、オープンデータ部とクローズドデータ部とから構成され、オープンデータ部とクローズドデータ部とは、それぞれ生産データ部、物流データ部、販売データ部、サービスデータ部、回収リサイクルデータ部から構成されている。

##### 【0077】

データベース61に記憶されている情報の一例を、図22に示す。この図に示すように、オープンデータ部の生産データ部には、「分解方法」、「部品データ」及び「有毒情報」が記憶されている。オープンデータ部の回収リサイクルデータ部には、「リサイクル活用情報」が記憶されている。

また、クローズドデータ部の生産データ部には、「検査情報」が記憶されている。物流データ部には、「追跡記録」が記憶されている。販売データ部には、「POS情報」及び「販売先情報」が記憶されている。サービスデータ部には、「品質情報」が記憶されている。回収リサイクルデータ部には、「マニフェスト情報」が記憶されている。

##### (2) DB更新部603

DB更新部603は、制御部601の指示により、データベース61に情報を

書込み、又は、データベース 61 から情報を読み出す。

### (3) 制御部 601

制御部 601 は、DB 更新部 603 を介して、データベース 61 に情報を書込み、又は、データベース 61 から情報を読み出す。

### 【0078】

また、LAN 接続部 602 を介して、管理装置 40 と接続され、管理装置 40 から情報を受け取り、データベース 61 に受け取った情報を書き込む。また、データベース 61 から読み出した情報を管理装置 40 へ出力する。

### (4) LAN 接続部 602

LAN 接続部 602 は、制御部 601 と LAN 装置 70 とを接続する。

### 1. 8 リーダライタ 30 及び無線 IC タグ 80 の動作

リーダーライタ 30 及び無線 IC タグ 80 の動作について説明する。

#### (1) リーダライタ 30 及び無線 IC タグ 80 の概要動作

リーダーライタ 30 及び無線 IC タグ 80 の概要動作について、図 23 に示すフローチャートを用いて説明する。

### 【0079】

同期信号送信期間において、制御部 102 は、同期信号送信命令を出力し、生成した同期信号波を出力し、命令生成部 104 は、同期信号送信命令に基づいて、パルス信号波を生成して出力し、同期信号波に基づいて、パルス信号波を生成して出力し、変復調部 111 は、搬送波の振幅を変化させ、振幅の変化した搬送波を出力し、アンテナ部 112 は、搬送波を電波として空間に放射する。制御部 209 は、アンテナ部 201、復調部 206、命令解読部 207 を介して、同期信号送信命令を受け取り、さらに同期信号波を受信し、同期信号を抽出し、抽出した同期信号に同期する同期信号を繰り返し含む同期信号波を生成する（ステップ S102）。

### 【0080】

制御部 102 は、識別コード収集命令を出力し、命令生成部 104 は、パルス信号波を生成して出力し、変復調部 111 は、搬送波の振幅を変化させ、振幅の変化した搬送波を出力し、アンテナ部 112 は、搬送波を電波として空間に放射

する。制御部 209 は、アンテナ部 201、復調部 206、命令解読部 207 を介して、識別コード収集命令を受け取る（ステップ S103）。

#### 【0081】

制御部 102 は、3 秒間の識別コード収集期間の経過を監視し（ステップ S104）、3 秒間の識別コード収集期間において、各無線 IC タグから識別コードを収集する（ステップ S105）。識別コード収集期間が経過すると（ステップ S104）、制御部 102 は、各無線 IC タグから識別コードの収集が終了したとみなし、識別コードの収集を終了する。

#### 【0082】

次に、アクセス期間において、制御部 102 は、識別コード記憶部 106 に記憶されている全ての識別コードの読み出しが終了するまで（ステップ S106）、各識別コードについて、各識別コードにより識別される無線 IC タグの領域アクセス認証と領域アクセスとを繰り返し行い（ステップ S107）、識別コード記憶部 106 に記憶されている全ての識別コードの読み出しが終了すると（ステップ S106）、処理を終了する。

#### （2）無線 IC タグの識別コードの収集の動作

ここでは、図 23 のフローチャートのステップ S105 に示す無線 IC タグの識別コードの収集の動作について、図 24 に示すフローチャートを用いて説明する。

#### 【0083】

制御部 209 は、乱数生成部 211 に対して乱数を生成するように指示し、乱数生成部 211 は、乱数 R0 を生成し（ステップ S131）、ハッシュ部 212 はハッシュ値を生成し、制御部 209 は、識別コード記憶部 208 から識別コードを読み出し、ハッシュ部 212 からハッシュ値を受け取り、受け取ったハッシュ値をチャネル番号とするチャネルを選択し（ステップ S132）、識別コード送信期間において、選択したチャネルにより（ステップ S133）、読み出した識別コードと乱数 R0 と識別コード送信命令とを変調部 213 及びアンテナ部 201 を介してリーダライタ 30 へ送信し、アンテナ部 112、変復調部 111 及び命令解読部 110 を介して、制御部 102 は、識別コード送信命令と識別コ



ドとを受け取り、ハッシュ部109は、乱数R0を受け取り（ステップS134）、ハッシュ部109は、ハッシュ値を生成し、制御部102は、受け取った識別コードを一時記憶部103に書き込み、生成されたハッシュ値をチャンネル番号とするチャンネルを選択し（ステップS135）、制御部102は、識別コード応答期間内の選択したチャンネルにおいて（ステップS136）、前記識別コードと識別コード応答命令とを命令生成部104、変復調部111及びアンテナ部112を介して送信し（ステップS138）、制御部209は、アンテナ部201、復調部206及び命令解読部207を介して、識別コード応答期間において、選択したチャンネルにより（ステップS137）、識別コード応答命令と識別コードとを受け取り（ステップS138）、制御部209は、識別コード記憶部208から読み出した識別コードと、受け取った識別コードとを比較し、一致しているなら（ステップS139）、識別コード一致期間において、選択したチャンネルにより（ステップS140）、識別コードと識別コード一致命令とを、変調部213及びアンテナ部201を介して出力する（ステップS142）。一致していないなら（ステップS140）、ステップS131へ戻って、処理を繰り返す。

#### 【0084】

制御部102は、識別コード一致期間内の選択したチャンネルにおいて（ステップS141）、アンテナ部112、変復調部111、命令解読部110を介して、識別コード一致命令を受け取り（ステップS142）、一時記憶部103から前記識別コード読み出し、読み出した識別コードを識別コード記憶部106へ書き込む（ステップS143）。

#### （3）無線ICタグの領域アクセス認証及び領域アクセスの動作

ここでは、図23のフローチャートのステップS107に示す無線ICタグの領域アクセス認証と領域アクセスの動作について、図25に示すフローチャートを用いて説明する。

#### 【0085】

制御部102は、アクセス期間において、識別コード記憶部106から1個の識別コードを読み出し（ステップS161）、アクセス要求命令と前記読み出した識別コードとを、命令生成部104、変復調部111及びアンテナ部112を

介して出力し、制御部209は、アクセス期間において、アンテナ部201、復調部206及び命令解読部207を介して、識別コードとアクセス要求命令とを受け取り（ステップS162）、制御部209は、受け取った識別コードと識別コード記憶部208から読み出した識別コードとを比較し、一致しなければ（ステップS163）、さらにアクセス要求命令の受け取りを待ち受ける。一致すれば（ステップS163）、制御部209は、乱数生成部211に対して乱数を生成するように指示し、乱数生成部211は、乱数R0を生成し（ステップS164）、暗号化部108は、鍵記憶部231から領域鍵K1～K6を読み出し、読み出した領域鍵K1～K6を用いて、乱数R0に暗号アルゴリズムE1を施して、それぞれ暗号化乱数R1～R6を生成し、生成した暗号化乱数R1～R6を生成乱数記憶部234に書き込む（ステップS166）。制御部209は、識別コードと乱数R0と認証子送信命令とを変調部213及びアンテナ部201を介して出力し、アンテナ部112、変復調部111及び命令解読部110を介して、制御部102は、認証子送信命令と識別コードとを受け取り、ハッシュ部109は、乱数R0を受け取り（ステップS165）、ハッシュ部109は、ハッシュ値を生成し、制御部102は、鍵記憶部107に記憶されている領域鍵を読み出し、暗号化部108は、乱数R0を領域鍵を用いて暗号化して暗号化乱数R0'を生成し（ステップS167）、制御部102は、命令生成部104へ前記識別コードと認証子応答命令とを出力し、命令生成部104は、暗号化乱数R0'と識別コードと認証子応答命令とを、変復調部111及びアンテナ部112を介して出力し、アンテナ部201及び復調部206を介して、命令解読部207は暗号化乱数R0'を受け取り、制御部209は、認証子応答命令と識別コードを受け取り、（ステップS168）、制御部209は、受け取った識別コードと識別コード記憶部208から読み出した識別コードとを比較し、一致しなければ（ステップS169）、さらに、認証子応答命令の受け取りを待ち受ける。一致すれば（ステップS169）、比較器235は、命令解読部207から受け取った暗号化乱数R0'に一致する暗号化乱数を生成乱数記憶部234から捜し、一致する暗号化乱数があれば（ステップS170）、一致する暗号化乱数を識別する番号Xiを制御部209へ出力する（ステップS172）。一致する暗号化乱数が

なければ（ステップS170）、比較器235は、暗号化乱数が一致しない旨を制御部209へ出力し、制御部209は、識別コードとアクセス不許可命令と理由コードとを、変調部213及びアンテナ部201を介して出力する（ステップS171）。

#### 【0086】

制御部102は、前記識別コードとアクセス情報とアクセス命令とを、命令生成部104、変復調部111及びアンテナ部112を介して出力し、制御部209は、アクセス命令と識別コードとアクセス情報とを、アンテナ部201、復調部206及び命令解読部207を介して受け取る（ステップS173）。制御部209は、次に、受け取った識別コードと識別コード記憶部208から読み出した識別コードとを比較し、一致しなければ（ステップS174）、さらに、アクセス命令の受け取りを待ち受ける。一致すれば（ステップS174）、制御部209は、アクセス情報に含まれる物理アドレスが番号Xiで示されるステージ領域内を示しているか否かを判断し、ステージ領域内を示していない場合には（ステップS175）、識別コードとアクセス不許可命令と理由コードとを、変調部213及びアンテナ部201を介して出力し、制御部102は、アンテナ部112、変復調部111及び命令解読部110を介して、識別コードとアクセス不許可命令と理由コードとを受け取る。

#### 【0087】

ステージ領域内を示している場合には（ステップS175）、制御部209は、アクセス命令とアクセス情報とを入出力部215へ出力し、入出力部215は、制御部209からアクセス命令とアクセス情報とを受け取り、アクセス命令とアクセス情報とに基づいてメモリ部216にアクセスを行い、制御部209は、そのアクセスの結果に基づいて、アクセス応答情報を生成し（ステップS177）、識別コードとアクセス応答命令とアクセス応答情報とを、変調部213及びアンテナ部201を介してへ出力し、制御部102は、アンテナ部112、変復調部111及び命令解読部110を介して、アクセス応答命令とアクセス応答情報と識別コードとを受け取り（ステップS178）、入出力部101は、アクセス応答命令とアクセス応答情報と識別コードとを受け取り、管理装置40へ受け

取ったアクセス応答命令とアクセス応答情報と識別コードとを出力する。

#### 1. 9 無線 I C タグの種類と適用分野

無線 I C タグ 8 0 は、搬送周波数として、2. 4 ~ 2. 5 G H z の準マイクロ波帯を使用し、電波方式により通信を行っている。

##### 【0088】

また、無線 I C タグ 8 0 は、8 6 0 M H z ~ 9 1 5 M H z の U H F 帯を使用し、同様に電波方式により通信を行うようにしてもよい。この場合、タグ寸法は、一例として、長さ 1 0 0 m m、幅 1 5 m m、厚さ 0. 5 m m である。このとき、通信可能な距離は、2 ~ 3 m であり、通信速度は、1 0 ~ 2 0 m 秒 / b y t e である。

##### 【0089】

この他に、磁気方式（電磁誘導方式）による無線 I C タグが知られており、使用される周波数は、1 2 5 K H z 又は 1 3. 5 6 M H z であり、寸法は、縦 6 c m、横 8 c m であり、通信距離は、5 0 c m 以内であり、通信速度は、数 K b p s である。また、重ね読みはできない、又は 3 枚程度以内まで可能である。

電波方式は、磁気方式よりも高周波を用いるので、アンテナを小さくでき、タグを小型化できる。

##### 【0090】

無線 I C タグの適用分野と、タグ単価と、通信距離との関係を図 2 6 に示す。この図では、横軸にタグ単価をとり、縦軸に通信距離をとっている。

タグ単価が数円から 5 0 0 円程度であり、通信距離が数 1 0 c m 以上である範囲 A 1 0 は、前記の電波方式を用いる無線 I C タグの適用範囲を示し、この範囲内における用途として、宅配 A 2 5、郵便 A 2 2、航空手荷物 A 2 3、洗濯物管理 A 2 4、ライフサイクルマネジメント A 2 1 及び車両管理 A 2 6 がある。

##### 【0091】

また、タグ単価が 1 0 円 ~ 5 0 0 円であり、通信距離が 5 0 c m 以内である範囲 A 1 1 は、前記磁気方式（1 3 M H z 帯）を用いる無線 I C タグの適用範囲を示し、この範囲内における用途として、O A 機器用消耗品管理 A 3 1、イモビライザ A 3 0、テレホンカード A 3 2 及び定期券 A 2 9 がある。

また、タグ単価が10円以下であり、通信距離が数10cm程度である範囲A27において、共振タグが知られており、万引き防止のために用いられている。

#### 1. 10 その他の変形例

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は上記実施の形態に限定されないのはもちろんである。すなわち、以下のような場合も本発明に含まれる。

(1) 図3に示す衣服90に付されている無線ICタグ80bは、図18に示すように、非プロテクト部のサービスステージ領域に、「洗濯方法」が記録されている。家庭用電気洗濯機500は、図27に示すように、洗濯槽内上部501において、リーダライタ30と同様のリーダライタを内蔵しており、また、様々な洗濯方法に応じた洗濯コースを記憶している。衣服90が洗濯槽内に入れられると、家庭用電気洗濯機500が内蔵するリーダライタは、無線ICタグ80bの非プロテクト部のサービスステージ領域に記録されている「洗濯方法」を読み出し、家庭用電気洗濯機500は、読み出した洗濯方法に応じた洗濯コースを読み出し、読み出した洗濯コースにより、洗濯を開始する。

#### 【0092】

また、食材に無線ICタグが添付され、この無線ICタグは、調理方法を非プロテクト部のサービスステージ領域に記憶しており、電子レンジなどの調理器は、リーダライタ30と同様のリーダライタを内蔵しており、また、様々な調理方法に応じた調理コースを記憶している。無線ICタグの添付された食材が内部に入れられると、調理器が内蔵するリーダライタは、無線ICタグの非プロテクト部のサービスステージ領域に記録されている「調理方法」を読み出し、調理器は、読み出した調理方法に応じた調理コースを読み出し、読み出した調理コースにより、食材を調理する。

(2) メモリ部216は、5個のステージ領域を有するとしているが、5個に限定されることはない。5個より多いステージ領域を有するとしてもよいし、5個より少ないステージ領域を有するとしてもよい。

#### 【0093】

また、無線ICタグ80のメモリ部216内の可変部は、この領域内に情報が

埋め尽くされれば、可変部の先頭から再度上書きするとしてもよい。

また、図28に示すように、非プロテクト部とプロテクト部とから構成され、プロテクト部は、生産ステージ領域と物流ステージ領域と販売ステージ領域とサービスステージ領域と回収リサイクルステージ領域と拡張領域とから構成されるとしてもよい。拡張領域は、各ステージ領域内が情報で埋め尽くされた場合に、さらに情報を書き込む領域として用いられる。

(3) リーダライタが、同一時間帯内において、1個の無線ICタグのみに対して読み書きを行う場合には、図23に示す処理を行う代わりに、図29に示すフローチャートに示すようにして、ステージ領域の認証とステージ領域へのアクセスを行うようにしてもよい。

#### 【0094】

リーダライタは、アクセス要求を無線ICタグに送信する(ステップS202)。無線ICタグは、乱数R0を生成し(ステップS203)、生成した乱数R0をリーダライタへ出力する(ステップS204)。リーダライタは、暗号化乱数 $R0' = E1(R0, K1)$ を生成し(ステップS206)、生成した暗号化乱数R0'を無線ICタグに送信する(ステップS207)。無線ICタグは、暗号化乱数 $R1 = E1(R0, K1)$ 、 $R2 = E1(R0, K2)$ 、・・・、 $R6 = E1(R0, K6)$ を生成し(ステップS205)、受け取った暗号化乱数R0'が、R1～R6のいずれかに一致するか否かを判断し、一致しない場合に(ステップS208)、「アクセス不許可」をリーダライタへ送信し(ステップS209)、一致する場合に(ステップS208)、ステージ領域を識別するXiを決定する(ステップS210)。リーダライタは、領域X3へのアクセスを行うアクセス命令を無線ICタグへ送信する(ステップS211)。無線ICタグは、XiとX3とが一致するか否かを判断し、一致しない場合に(ステップS212)、リーダライタに「アクセス不許可」を送信する(ステップS213)。一致する場合に(ステップS212)、前記アクセス命令に基づいて無線ICタグが有するメモリにアクセスし(ステップS214)、アクセス結果をアクセス応答としてリーダライタへ送信する(ステップS215)。

(4) 無線ICタグ80は、上記に説明したように、搬送周波数として、2.4

～2. 5 G H z の準マイクロ波帯を使用し、電波方式により通信を行うとしているが、搬送周波数として、2. 4 ～2. 5 G H z の準マイクロ波帯及び8 6 0 M H z ～9 1 5 M H z のU H F 帯の両方を使用し、同様に電波方式により通信を行うとしてもよい。

【0 0 9 5】

また、無線 I C タグ 8 0 を使用するステージに応じて、リーダライタ 3 0 は、使用する搬送周波数として U H F 帯又は準マイクロ波帯のいずれかを選択するようにしてもよい。例えば、リーダライタ 3 0 と無線 I C タグ 8 0 との距離が一定して近接している生産工場内においては、通信距離の短い準マイクロ波帯を選択し、リーダライタ 3 0 と無線 I C タグ 8 0 との距離が一定しないと考えられる物流ステージ内においては、通信距離の長い U H F 帯を選択するようにしてもよい。

(5) 上記の実施の形態においては、同一期間において複数の無線 I C タグへのアクセスを行うマルチ読み取りを行う際に、識別コード収集期間において、時分割方式により識別コードを収集し、アクセス期間においては、リーダライタ 3 0 は、各無線 I C タグについて順番にアクセスするとしているが、アクセス期間においても時分割方式により、リーダライタ 3 0 は、各無線 I C タグにアクセスするとしてもよい。

【0 0 9 6】

また、識別コード収集期間は、第 1 収集期間と第 2 収集期間との 2 個の収集期間を含み、第 1 収集期間と第 2 収集期間とにおいて、識別コードを収集するとしているが、識別コード収集期間は、3 個以上の収集期間を含み、それぞれの収集期間において、識別コードを収集するとしてもよい。

また、搬送周波数として、2. 4 ～2. 5 G H z の準マイクロ波帯を周波数分割して、分割された各周波数を複数の無線 I C タグに割り当てて、リーダライタ 3 0 は、分割された各周波数を用いて、各無線 I C タグにアクセスするとしてもよい。

【0 0 9 7】

また、スペクトラム拡散技術に基づく CDMA (C o d e D i v i s i o n

M u l t p l e   A c c e s s ) 方式を用いるとしてもよい。無線 I C タグ毎にそれぞれ異なる拡散コードを設定し、複数の無線 I C タグが同一の広帯域無線チャネルを共有する。

また、リーダライタ 3 0 と各無線 I C タグとの間で通信する情報をパケットデータに分割し、各パケットデータの先頭に各無線 I C タグを識別する識別コードを付加し、リーダライタ 3 0 は、パケットデータを用いて、各無線 I C タグにアクセスするとしてもよい。

( 6 ) 識別コードは、3 2 ビットからなり、製造業者識別コード ( 1 0 ビット長 ) と、種類コード ( 1 0 ビット長 ) と、製造番号 ( 1 2 ビット長 ) とから構成されるとしているので、2 の 3 2 乗個分の識別コードを生成できる。

[ 0 0 9 8 ]

さらに、多くの数の識別コードが必要であれば、識別コードのビット長を増やすとしてもよい。

また、識別コードを 3 2 ビット長とし、さらに、多くの数の識別コードが必要であれば、3 2 ビット長の乱数を生成し、生成した乱数と 3 2 ビットの前記識別コードとを加算して、3 2 ビット長の加算結果を得、得られた加算結果を識別コードとしてもよい。この識別コードを用いて無線 I C タグとリーダライタとの間で通信を行うとしてもよい。リーダライタ 3 0 により無線 I C タグ 8 0 にアクセスする場合に、識別コードは、最大 5 0 個の無線 I C タグを識別できればよいからである。ここで、もちろん加算以外の他の演算を用いるとしてもよい。

( 7 ) 無線 I C タグ 8 0 及びリーダライタ 3 0 は、記憶している領域鍵が漏洩しないように、無線 I C タグ 8 0 及びリーダライタ 3 0 が記憶している領域鍵を不正に読みだそうとして、無線 I C タグ 8 0 及びリーダライタ 3 0 を分解すると、前記領域鍵を記憶しているメモリが破壊されるタンパ方式を採用するとしてもよい。

( 8 ) さらに、領域鍵配信装置を設け、領域鍵配信装置は、無線 I C タグ 8 0 と接続され、6 個の領域鍵 ( K 1 ~ K 6 ) を無線 I C タグ 8 0 内部に書き込むとしてもよい。また、領域鍵配信装置は、リーダライタ 3 0 と接続され、2 個の領域鍵 ( K 1 及び K 6、K 2 及び K 6、K 3 及び K 6、K 4 及び K 6 又は K 5 及び



K 6の何れか) をリーダライタ 30 内に書き込むとしてもよい。

【0099】

この領域鍵配信装置は、リーダライタ 30 及び無線 IC タグ 80 の製造業者以外の第三者機関が所有し、この第三者機関によりこの領域鍵配信装置を用いて、リーダライタ 30 及び無線 IC タグ 80 にそれぞれ領域鍵が書き込まれるとしてもよい。これにより、領域鍵のリーダライタ 30 及び無線 IC タグ 80 への書込み時点での、領域鍵の漏洩を防ぐことができる。

(9) すべての領域にアクセスを許すオールマイティ鍵 K 7 を設け、特別に許された使用者のみにより使用されるリーダライタ 30 内部にオールマイティ鍵 K 7 を有し、オールマイティ鍵 K 7 により無線 IC タグ 80 の全ての領域へのアクセスが可能であるとしてもよい。また、前記第三者機関がこの使用者であるとしてもよい。

(10) 上記の実施の形態では、無線 IC タグがリーダライタを認証するとしているが、図 25 に示すフローチャートのステップ S 161 ~ S 170 において、リーダライタの処理と無線 IC タグの処理とを逆にすることにより、リーダライタが無線 IC タグを認証するとしてもよい。これにより、不正に製造された無線 IC タグをリーダライタは拒否することができる。

【0100】

また、無線 IC タグがリーダライタを認証し、かつリーダライタが無線 IC タグを認証するとしてもよい。

(11) 販売ステージ領域には、WPC コード (JAN、EAN、UPC コード) を記録するようにしてもよい。ここで、EAN (EUROPEAN ARTICLE NUMBERING SYSTEM) は、ヨーロッパで使用されている小売食品外装用の国際的な標準コード体系である。UPC (Universal Product Code) は、米国での小売り食品包装用標準バーコードシンボルである。また、JAN は、1978 年に JIS 化された共通商品コードで日本で使用されているコード体系である。

(12) リーダライタは、さらにバーコードを読むように構成してもよい。

【0101】

また、無線ＩＣタグの樹脂表面にバーコードを印刷して、バーコードの印刷された無線ＩＣタグを製品表面に貼り付けるようにしてもよい。このバーコードの印刷された無線ＩＣタグについて、前記リーダライタは前記バーコードを読み、また、無線ＩＣタグにアクセスするようにしてもよい。

(13) 無線ＩＣタグの貼り付け位置は、ロゴ裏面に限定されない。例えば、テレビジョン受像機の内部に設けられた配線基板の上面に無線ＩＣタグを貼り付けるとしてもよい。このように、無線ＩＣタグの貼り付け位置は、リーダライタ30から送信される電波の届く製品の内部であってもよい。

(14) 商店で陳列されている商品に無線ＩＣタグを添付し、商店のレジにリーダライタ30と同様の構成を有する第1のリーダライタを設置し、第1のリーダライタは、正当に対価が支払われた商品に添付されている無線ＩＣタグにその旨を記録し、商店の出入り口にリーダライタ30と同様の構成を有する第2のリーダライタを設置し、第2のリーダライタは、無線ＩＣタグに前記の旨が記録されていない無線ＩＣタグを検出する。これにより、商品の万引きを防止することができる。

(15) 衣服の製造業者は、その製造業者名を記録している無線ＩＣタグを製造した衣服に添付し、仕入れ業者は、無線ＩＣタグに記録されている製造業者名をリーダライタ30により読み出すことにより、衣服の製造業者名を確認することができる。これにより、ニセモノを誤って購入することを防止できる。

#### 【0102】

また、高級衣料品や高級装飾品などの高級ブランド品に、無線ＩＣタグを添付することにより、高級ブランド品の偽物の流通を防止することができる。また、高級ブランド品の品質を保証することができる。また、流通経路において、経路情報を無線ＩＣタグに書き込むことにより、流通の経路の管理、探索ができる。

(16) 生産現場において、生産従事者は、その者の名前が記録されている無線ＩＣタグが裏面に添付されている名札を身につけ、生産現場の各所において、リーダライタ30と同様の構成を有するリーダライタが設置され、このリーダライタは、無線ＩＣタグに記録されてる名前を読み出し、その場所とともに記録する。これにより、生産現場における人の動きの管理をすることができる。また、小

売店などにおいても同様である。

(17) 病院において、患者が入院し、治療を受け、退院に至るまでにおいて、上記の製品のライフサイクルと同様に、病院の療養サイクルにおける複数のステージ、すなわち、入院、検査、手術、治療、養生、投薬、会計、退院などを経る。これらの複数のステージ毎に、それぞれ必要な情報が存在する。

#### 【0103】

患者は、無線ICタグを身につける。無線ICタグは、ステージ毎のステージ領域を有している。入院ステージ領域には、患者の名前及び病状情報が書き込まれ、検査ステージ領域には、検査結果が書き込まれ、手術ステージ領域には、手術方法及び結果が書き込まれ、治療ステージ領域には、治療方法及び結果などの処置情報が書き込まれ、養生ステージ領域には、養生中の病状情報が書き込まれ、投薬ステージ領域には、患者に投薬された医薬品に関する情報が書き込まれ、会計ステージ領域には、治療、投薬などの保険点数及び金額情報が書き込まれ、退院ステージ領域には、退院時点における病状情報が書き込まれている。各ステージ領域にアクセスできる権限を有する者は限定されている。病院内の病室、治療室、手術室、会計室などの各所において、リーダライタ30と同様の構成を有する各ステージのリーダライタが設置され、各ステージのリーダライタを操作する権限を有する者、例えば、患者、医者、看護者又は会計担当者などは、自分だけが秘密に知っているパスワードをリーダライタに入力し、正しく権限を有する者である場合には、リーダライタは、無線ICタグの各ステージ領域から情報を読み出し、又は情報を書き込む。

#### 【0104】

これにより、患者は、自分の病状や治療方法について正しい知識を得ることができる。また、医者又は看護者が患者を取り違えたり、処置を誤ったりすることを防止ができる。また、会計担当者は、正確に治療代金などを計算できる。

(18) 物流ステージにおいて、図7に示すように、物流管理サブシステム20bに含まれる第3組のリーダライタ30d及び携帯電話内蔵型管理装置40dが、貨物トラックに搭載され、アンテナ部を有するリーダライタ30dが、貨物トラックの荷物搬入口の上部内側に設置されているので、荷物搬入口近辺の無線I

Cタグの添付された貨物の内容物を無線ICタグに記録されている情報を読み出すことにより知ることができる。こうして得られた貨物の内容物についての情報と現在トラックが位置している場所の情報とを、基地局50、公衆回線、受信装置51、接続装置53、LAN装置70を介して、ホストコンピュータ60のデータベース61に書き込む。

## 【0105】

これにより、貨物トラックに搬入された貨物又は貨物トラックから搬出された貨物の内容物とその位置とを時々刻々と知ることができるので、貨物の流通ルートを確実に把握することができる。

(19) 無線ICタグが本、CD、衣服などに添付され、これらの本、CD、衣服などが重なり合って保管されている場合においても、リーダライタ30は、これら複数の無線ICタグとのアクセスを行うことができるので、これらの本、CD、衣服などの在庫管理ができる。

(20) オフィ스에 複数台設置されているコンピュータやプリンタなどを接続する複数の配線毎に、前記配線が接続する機器と機器とを示す情報が記録されている無線ICタグを添付し、これらの複数の配線をオフィスの床下に埋め込む。

## 【0106】

リーダライタを床上から操作して、これらの無線ICタグに記録されている情報を読み出すことにより、機器と機器とを接続する配線の位置を知ることができる。

(21) 自動車の車体に無線ICタグを添付し、サービスステージ領域に、自動車の運行状況、例えば、走行距離数と日付、給油量と日付などを定期的に無線ICタグに記録するようにしてもよい。また、自動車の修理履歴を記録して管理するようにしてもよい。また、自動車が廃車とされたときに、これらの情報を用いて、自動車の部品、モジュールのリユースを決定するようにしてもよい。

## 【0107】

このようにして、廃棄される物品のリユースが簡単に決定できるので、廃棄される物品の回収率が向上し、さらに、物品が再利用されるリユース率が向上する。

(22) 無線 IC タグに、さらに、温度センサ、圧力センサなどのセンサを付加し、これらのセンサにより、定期的に、無線 IC タグの周辺の温度、圧力などを検出し、検出した温度、圧力などを無線 IC タグ内に記録するようにしてもよい。また、この無線 IC タグは、これらのセンサを駆動させるため電池を備えているとしてもよい。

(23) 家庭内に用いられる電化製品や衣服に無線 IC タグが添付され、リーダーライタを用いて、家庭内に存在するこれらの電化製品や衣服に添付されている無線 IC タグに記録されている情報を読み出すことにより、家庭内資産管理を行うことができる。

(24) 上記実施の形態では、秘密鍵方式による暗号を用いているが、公開鍵方式による暗号を用いるとしてもよい。例えば、楕円曲線上の離散対数問題を安全性の根拠とする暗号通信方式を用いてもよい。

(25) 本発明は、本実施の形態に示す方法であるとしてもよい。

#### 【0108】

また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

#### 【0109】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

(26) 本発明は、上記に示す実施の形態、複数の変形例、又は上記実施の形態及び複数の変形例の一部を組み合わせたとしてもよい。

#### 【0110】

## 【発明の効果】

上記に説明したように、本発明は、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な情報記憶媒体であって、複数の記憶領域を有する記憶手段と、各記憶領域を識別する識別子を格納している格納手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記格納手段に格納されている識別子のいずれかと一致するか否かを判断する判断手段と、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別される記憶領域へのアクセスを行う入出力手段とを備える。

## 【0111】

この構成によると、秘密に受信したアクセス識別子により識別される記憶領域に対して、アクセス装置はアクセスすることができるので、1個の情報記憶媒体を複数の目的において共用できるという効果がある。

また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグであって、前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段とを備える。

## 【0112】

この構成によると、秘密に受信したステージ識別子により識別されるステージ記憶領域に対して、アクセス装置はアクセスすることができるので、生産から廃棄に至るまでのライフサイクルにおける複数のステージにおいて、1個の非接触

ＩＣタグを、共用できるという効果がある。

ここで、前記秘密受信手段は、第１認証子を生成し、生成した第１認証子を前記アクセス装置へ出力する認証子出力手段と、前記アクセス識別子を暗号化鍵として用いて、出力した前記第１認証子に暗号アルゴリズムが施されて生成された第２認証子を前記アクセス装置から取得する取得手段と、前記複数のステージ識別子を暗号化鍵として用いて、生成した前記第１認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第３認証子を生成する暗号手段とを含み、前記判断手段は、取得した第２認証子が生成した複数の第３認証子のうちのいずれか１個と一致するか否かを判断し、一致する場合に、受信した前記アクセス識別子が前記識別子記憶手段に格納されているステージ識別子のいずれかと一致すると判断し、前記入出力手段は、前記アクセス識別子により識別されるステージ記憶領域として、前記第２認証子に一致する第３認証子を生成する際に暗号化鍵として用いられたステージ識別子により識別されるステージ記憶領域へのアクセスを行うように構成してもよい。

#### 【 0 1 1 3 】

この構成によると、非接触ＩＣタグは、ステージ識別子を送信されることなく、アクセス装置を認証するので、ステージ識別子が外部に漏れることがないという効果がある。

ここで、前記認証子出力手段は、ランダムに第１認証子を生成するように構成してもよい。

#### 【 0 1 1 4 】

この構成によると、非接触ＩＣタグは、ランダムに認証子を生成するので、過去の通信により、ステージ識別子が外部に漏れることがないという効果がある。

ここで、前記秘密受信手段は、時分割多重された通信チャネルのうち、１個の通信チャネルを選択するチャネル選択手段と、選択された前記通信チャネルを介して、アクセス識別子を秘密に受信する識別子受信手段とを含むように構成してもよい。

#### 【 0 1 1 5 】

この構成によると、非接触ＩＣタグは、時分割された通信チャネルを用いて、

アクセス装置と通信を行うので、アクセス装置は、同一時間帯において、複数の  
 う非接触 I C タグと通信を行うことができるという効果がある。

ここで、前記チャネル選択手段は、時分割多重された通信チャネルのうち、1  
 個の通信チャネルをランダムに選択するように構成してもよい。

#### 【 0 1 1 6 】

この構成によると、非接触 I C タグは、ランダムに時分割された通信チャネル  
 を選択するので、非接触 I C タグ同士で通信チャネルが重なる可能性が少なくな  
 るという効果がある。

ここで、前記記憶手段は、さらに、共有識別子により識別される共有記憶領域  
 を有し、前記識別子記憶手段は、さらに、前記共有識別子を記憶しており、前記  
 判断手段は、さらに、受信した前記アクセス識別子が前記識別子記憶手段に記憶  
 されている共有識別子と一致するか否かを判断し、前記アクセス情報受信手段は  
 、さらに、一致すると判断される場合に、前記アクセス装置からアクセス情報を  
 受信し、前記入出力手段は、さらに、受信したアクセス情報に基づいて、前記ア  
 クセス識別子により識別される共有記憶領域へのアクセスを行うように構成して  
 もよい。

#### 【 0 1 1 7 】

この構成によると、非接触 I C タグは、共有識別子により識別される共有領域  
 を有しているので、複数のステージにおいて、同じ情報を共用できるという効果  
 がある。

ここで、前記非接触 I C タグが有する不揮発性メモリは、ヒューズメモリであ  
 るとしてもよい。

#### 【 0 1 1 8 】

この構成によると、データの改竄を防ぐことができる。

また、本発明は、入院から退院に至るまでの病院の療養サイクルにおける複数  
 のステージを経由する入院患者に付され、不揮発性メモリを有し、電波を用いて  
 非接触に読み書き可能な非接触 I C タグであって、前記療養サイクルを構成する  
 ステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステー  
 ジ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と



、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段とを備える。

#### 【0119】

この構成によると、各ステージのリーダライタを操作する権限を有する者、例えば、患者、医者、看護者又は会計担当者などは、自分だけが秘密に知っているパスワードをリーダライタに入力し、正しく権限を有する者である場合には、リーダライタは、無線ＩＣタグの各ステージ領域から情報を読み出し、又は情報を書き込む。これにより、患者は、自分の病状や治療方法について正しい知識を得ることができる。また、医者又は看護者が患者を取り違えたり、処置を誤ったりすることを防止ができる。また、会計担当者は、正確に治療代金などを計算できる。

#### 【0120】

また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する高級ブランド品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ＩＣタグであって、前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段と、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信手段と、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断手段と、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信手段と、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力手段とを備える。

#### 【0121】

この構成によると、高級ブランド品の偽物の流通を防止することができる。ま

た、高級ブランド品の品質を保証することができる。また、流通経路において、経路情報を無線 I C タグに書き込むことにより、流通の経路の管理、探索ができる。

また、本発明は、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別される複数個の記憶領域を有し、電波を用いて非接触に読み書き可能な情報記憶媒体に対して情報を送受信するアクセス装置であって、アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子を暗号を用いて秘密に前記情報記憶媒体に対して送信する秘密送信手段と、前記情報記憶媒体により、秘密に送信した前記アクセス識別子が前記情報記憶媒体が有する複数個の記憶領域うちの 1 個の記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備える。

#### 【 0 1 2 2 】

この構成によると、秘密に受信したアクセス識別子により識別される記憶領域を有する情報記憶媒体に対して、アクセス装置はアクセスすることができるので、1 個の情報記憶媒体を複数の目的において共用できるという効果がある。

また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触 I C タグに対して情報を送受信するアクセス装置であって、アクセス識別子を記憶している識別子記憶手段と、前記アクセス識別子を暗号を用いて秘密に前記非接触 I C タグに対して送信する秘密送信手段と、前記非接触 I C タグにより、秘密に送信した前記アクセス識別子が前記非接触 I C タグが有する複数個のステージ記憶領域うちの 1 個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信手段とを備える。

#### 【 0 1 2 3 】

この構成によると、秘密に受信したステージ識別子により識別されるステージ記憶領域を有する非接触 I C タグに対して、アクセス装置はアクセスすることができるので、生産から廃棄に至るまでのライフサイクルにおける複数のステージ

において、1個の非接触ICタグを、共用できるという効果がある。

ここで、前記非接触ICタグは、前記複数個のステージ記憶領域をそれぞれ識別するステージ識別子を記憶しており、前記秘密送信手段は、前記非接触ICタグから第1認証子を受信する認証子受信手段と、前記アクセス識別子を暗号鍵として用いて、受信した前記第1認証子に暗号アルゴリズムを施して第2認証子を生成し、生成した第2認証子を前記非接触ICタグへ出力する認証子出力手段とを備え、前記アクセス情報送信手段は、前記非接触ICタグにより、前記複数のステージ識別子を暗号化鍵として用いて、前記第1認証子に前記暗号アルゴリズムと同じ暗号アルゴリズムを施して、複数の第3認証子が生成され、出力された前記第2認証子が生成した複数の第3認証子のうちのいずれか1個と一致するかどうか判断され、一致する場合に、前記アクセス識別子が前記複数個のステージ記憶領域うちの1個のステージ記憶領域を正しく識別すると判断されるときに、さらにアクセス情報を送信するように構成してもよい。

#### 【0124】

この構成によると、ステージ識別子を秘密に非接触ICタグに対して送信することなく、非接触ICタグにより認証されるので、ステージ識別子が外部に漏れることがないという効果がある。

また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成されライフサイクルを構成するステージ数と同数のステージ記憶領域を備え、電波を用いて非接触に読み書き可能な非接触ICタグと前記非接触ICタグに対して情報を送受信するアクセス装置とから構成されるアクセスシステムであって、前記非接触ICタグと、前記アクセス装置とから構成される。

#### 【0125】

この構成によると、上記に示す非接触ICタグ及びアクセス装置と同様の効果を奏することは明らかである。

また、本発明は、不揮発性メモリを有し、電波を用いて非接触に読み書き可能な非接触ICタグが付された物品が、生産から廃棄に至るまでの複数ステージを流通する物品ライフサイクルにおいて、ステージ毎に設けられたアクセス装置に

より前記非接触 I C タグにアクセスすることにより、前記物品を管理するライフサイクル管理システムであって、前記非接触 I C タグと、前記アクセス装置とを含み、ステージ毎に設けられたアクセス装置により、前記非接触 I C タグが有し、当該ステージに対応する 1 のステージ記憶領域にのみアクセスすることにより、前記物品を管理する。

#### 【 0 1 2 6 】

この構成によると、ステージ毎に設けられたアクセス装置により、前記非接触 I C タグが有し、当該ステージに対応する 1 のステージ記憶領域にのみアクセスすることにより、前記物品を管理するので、各ステージにおいて、上記に示す非接触 I C タグ及びアクセス装置と同様の効果を奏することは明らかである。

また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリを有し、電波を用いて非接触に読み書き可能であり、前記ライフサイクルを構成するステージ数と同数のステージ記憶領域を有する記憶手段と前記複数のステージ記憶領域をそれぞれ識別するステージ識別子を記憶している識別子記憶手段とを備える非接触 I C タグにより用いられる入出力方法であって、外部のアクセス装置から暗号を用いてアクセス識別子を秘密に受信する秘密受信ステップと、受信した前記アクセス識別子が前記識別子記憶手段に記憶されているステージ識別子のいずれかと一致するか否かを判断する判断ステップと、一致すると判断される場合に、前記アクセス装置からアクセス情報を受信するアクセス情報受信ステップと、受信したアクセス情報に基づいて、前記アクセス識別子により識別されるステージ記憶領域へのアクセスを行う入出力ステップとを含む。

#### 【 0 1 2 7 】

この方法を用いると、前記非接触 I C タグと同様の効果を奏することは明らかである。

また、本発明は、生産から廃棄に至るまでのライフサイクルにおける複数のステージを流通する物品に付され、不揮発性メモリにより構成され秘密の識別子によりそれぞれ識別されライフサイクルを構成するステージ数と同数のステージ記憶領域を有し、電波を用いて非接触に読み書き可能な非接触 I C タグに対して情

報を送受信し、アクセス識別子を記憶している識別子記憶手段を備えるアクセス装置により用いられるアクセス方法であって、前記アクセス識別子を暗号を用いて秘密に前記非接触 I C タグに対して送信する秘密送信ステップと、前記非接触 I C タグにより、秘密に送信した前記アクセス識別子が前記非接触 I C タグが有する複数のステージ記憶領域うちの 1 個のステージ記憶領域を正しく識別すると判断される場合に、さらにアクセス情報を送信するアクセス情報送信ステップとを含む。

#### 【 0 1 2 8 】

この方法を用いると、前記アクセス装置と同様の効果を奏することは明らかである。

#### 【図面の簡単な説明】

##### 【図 1】

生産 1、物流 2、販売 3、サービス 4、回収リサイクル 5 の各ステージを経て流通し、その一生を終える、製品の生産から廃棄・回収に至るまでの製品のライフサイクル 6 を示す。

##### 【図 2】

テレビ受像機の前面枠部分に、無線 I C タグが貼り付られ、無線 I C タグの上面に、ロゴマークが貼り付けられている状態を示す。

##### 【図 3】

無線 I C タグが貼り付けられたラベルが衣服の襟裏側部に縫い付けられている状態を示す。

##### 【図 4】

ライフサイクル管理システム 1 0 の構成を示すブロック図である。

##### 【図 5】

サブシステム 2 0 の構成を示すブロック図である。

##### 【図 6】

生産管理サブシステム 2 0 a に含まれる第 1 組のリーダーライタ 3 0 a 及び管理装置 4 0 a が、生産工場内に設置されている状況を示す。

##### 【図 7】

物流管理サブシステム 2 0 b に含まれる第 3 組のリーダライタ 3 0 d 及び携帯電話内蔵型管理装置 4 0 d が、貨物トラックに搭載されている様子を示す。

【図 8】

物流管理サブシステム 2 0 b に含まれる第 2 組の携帯電話型リーダライタ 3 0 c の外観を示す。

【図 9】

販売管理サブシステム 2 0 c に含まれる第 1 組のリーダライタ 3 0 b の外観を示す。

【図 1 0】

サービス管理サブシステム 2 0 d に含まれる第 4 組の携帯端末型リーダライタ 3 0 e の外観を示す。

【図 1 1】

リーダライタ 3 0 の構成を示すブロック図である。

【図 1 2】

同期信号送信期間、識別コード収集期間及びアクセス期間を示す。

【図 1 3】

命令生成部 1 0 4 が受け取る命令とこれらの命令に付随するオペランド等を示す。

【図 1 4】

命令解読部 1 1 0 が抽出する命令とオペランドとを示す。

【図 1 5】

無線 I C タグ 8 0 の外観を示す。

【図 1 6】

無線 I C タグ 8 0 の I C チップ部 2 0 0 の構成を示すブロック図である。

【図 1 7】

メモリ部 2 1 6 の構成を示すメモリマップである。

【図 1 8】

メモリ部 2 1 6 の構成を示すメモリマップである。メモリ部 2 1 6 の内容をステージ領域毎に示している。

## 【図 1 9】

電源部 2 0 3 に含まれる電源回路の一例を示す。

## 【図 2 0】

認証部 2 1 0 の構成を示すブロック図である。

## 【図 2 1】

管理装置 4 0 の構成及びホストコンピュータ 6 0 の構成を示すブロック図である。

## 【図 2 2】

ホストコンピュータ 6 0 のデータベース 6 1 に記憶されている情報の一例を示す。

## 【図 2 3】

リーダライタ 3 0 及び無線 I C タグ 8 0 の概要動作を示すフローチャートである。

## 【図 2 4】

無線 I C タグの識別コードの収集の動作を示すフローチャートである。

## 【図 2 5】

無線 I C タグの領域アクセス認証と領域アクセスの動作を示すフローチャートである。

## 【図 2 6】

無線 I C タグの適用分野と、タグ単価と、通信距離の関係を示す。

## 【図 2 7】

リーダライタ 3 0 と同様のリーダライタを内蔵している家庭用電気洗濯機の外觀図である。

## 【図 2 8】

拡張領域を含むメモリ部のメモリマップの一例である。

## 【図 2 9】

リーダライタが 1 個の無線 I C タグのみに対して読み書きを行う場合の、ステージ領域の認証とステージ領域へのアクセスの動作を示すフローチャートである。

【符号の説明】

- 10     ライフサイクル管理システム
- 20     サブシステム
- 20a   生産管理サブシステム
- 20b   物流管理サブシステム
- 20c   販売管理サブシステム
- 20d   サービス管理サブシステム
- 20e   回収リサイクル管理サブシステム
- 30     リーダライタ
- 30a   リーダライタ
- 30b   リーダライタ
- 30c   携帯電話型リーダライタ
- 30d   リーダライタ
- 30e   携帯端末型リーダライタ
- 40     管理装置
- 40a   管理装置
- 40d   携帯電話内蔵型管理装置
- 40e   管理装置
- 51     受信装置
- 52     ICカード
- 53     接続装置
- 60     ホストコンピュータ
- 61     データベース
- 70     LAN装置
- 80     無線ICタグ
- 80a   無線ICタグ
- 80b   無線ICタグ
- 101   入出力部
- 102   制御部

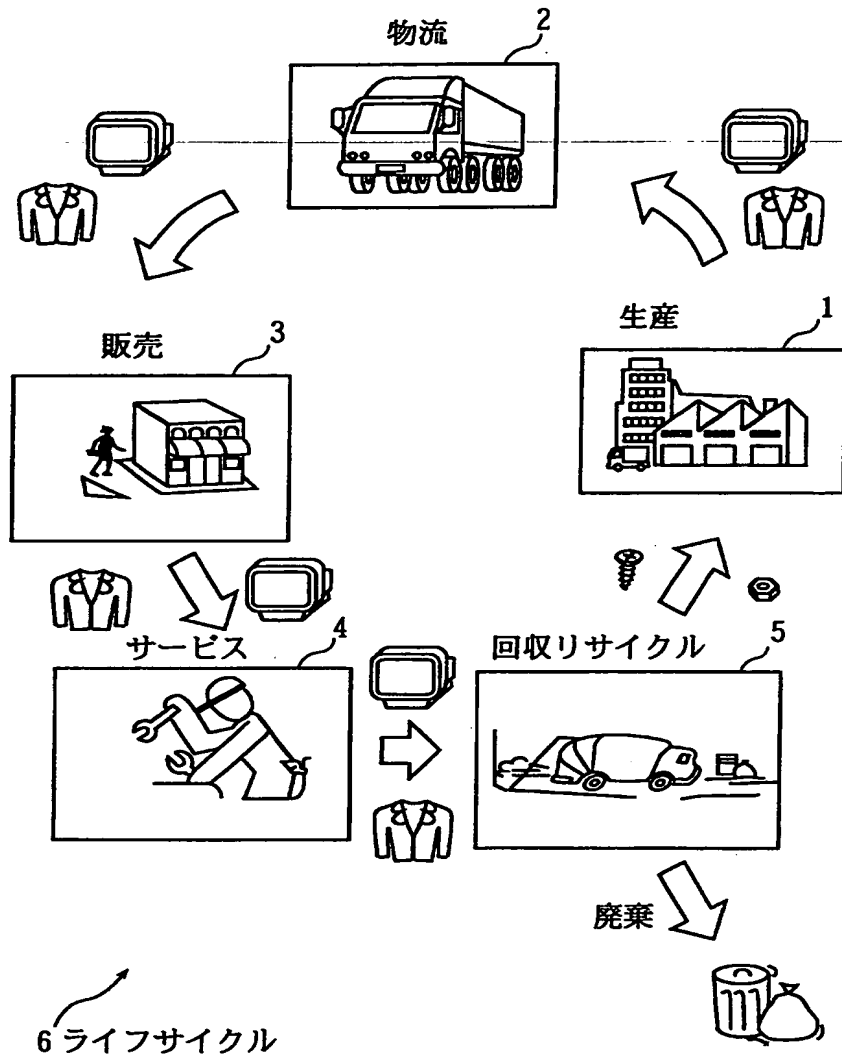


1 0 3	一時記憶部
1 0 4	命令生成部
1 0 5	クロック生成部
1 0 6	識別コード記憶部
1 0 7	鍵記憶部
1 0 8	暗号化部
1 0 9	ハッシュ部
1 1 0	命令解読部
1 1 1	変復調部
1 1 2	アンテナ部
2 0 0	I C チップ部
2 0 1	アンテナ部
2 0 3	電源部
2 0 6	復調部
2 0 7	命令解読部
2 0 8	識別コード記憶部
2 0 9	制御部
2 1 0	認証部
2 1 1	乱数生成部
2 1 2	ハッシュ部
2 1 3	変調部
2 1 4	クロック生成部
2 1 5	入出力部
2 1 6	メモリ部
2 3 1	鍵記憶部
2 3 2	乱数記憶部
2 3 3	暗号化部
2 3 4	生成乱数記憶部
2 3 5	比較器

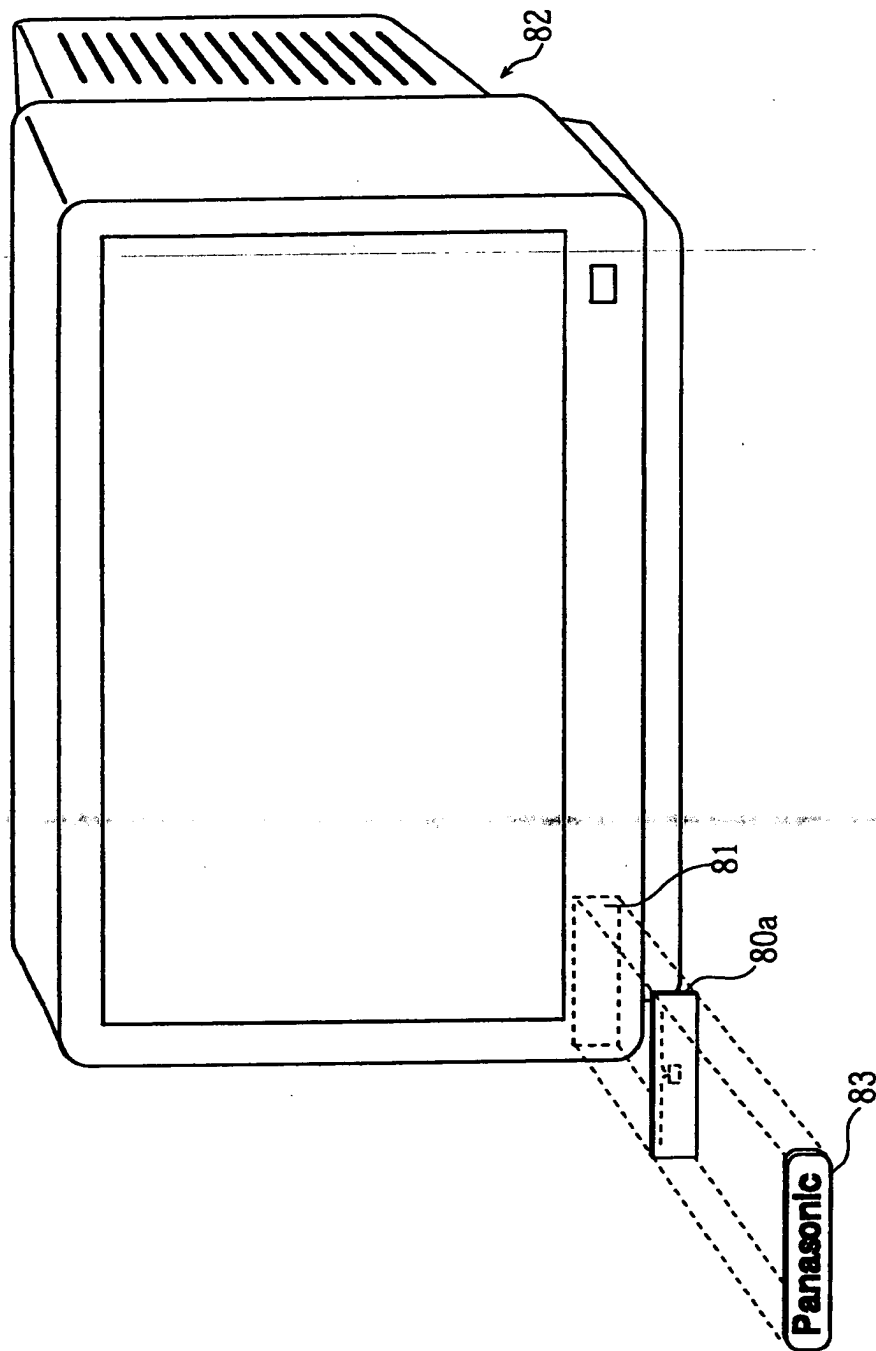
4 0 1	情報記憶部
4 0 2	制御部
4 0 3	L A N 接続部
4 0 4	入出力部
6 0 1	制御部
6 0 2	<u>L A N 接続部</u>
6 0 3	D B 更新部

【書類名】 図面

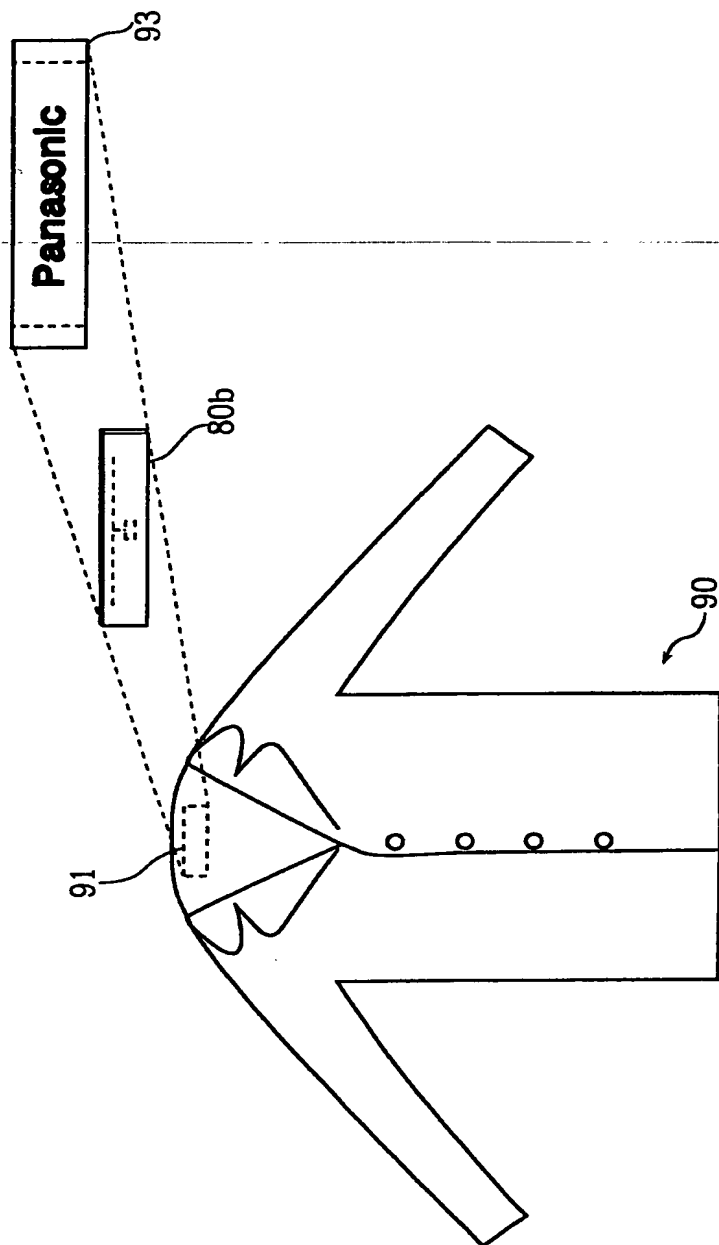
【図1】



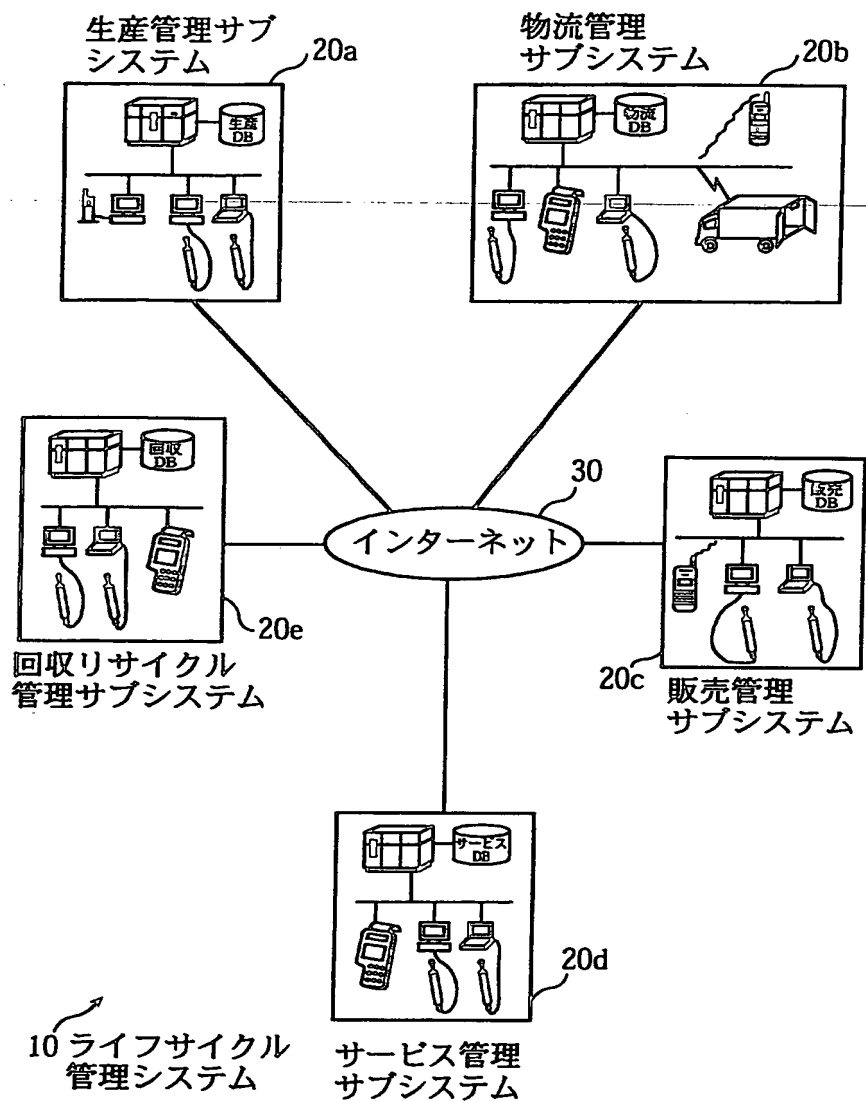
【図 2】



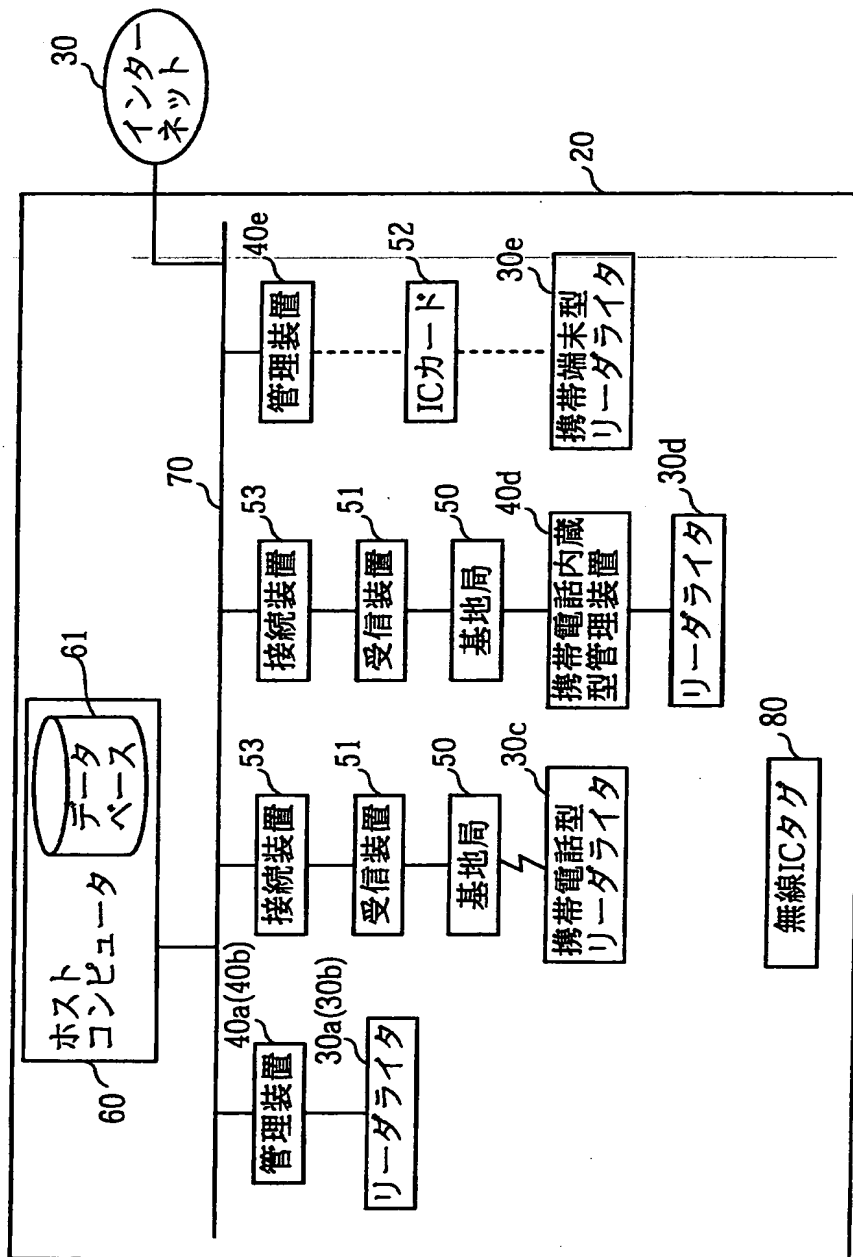
【図 3】



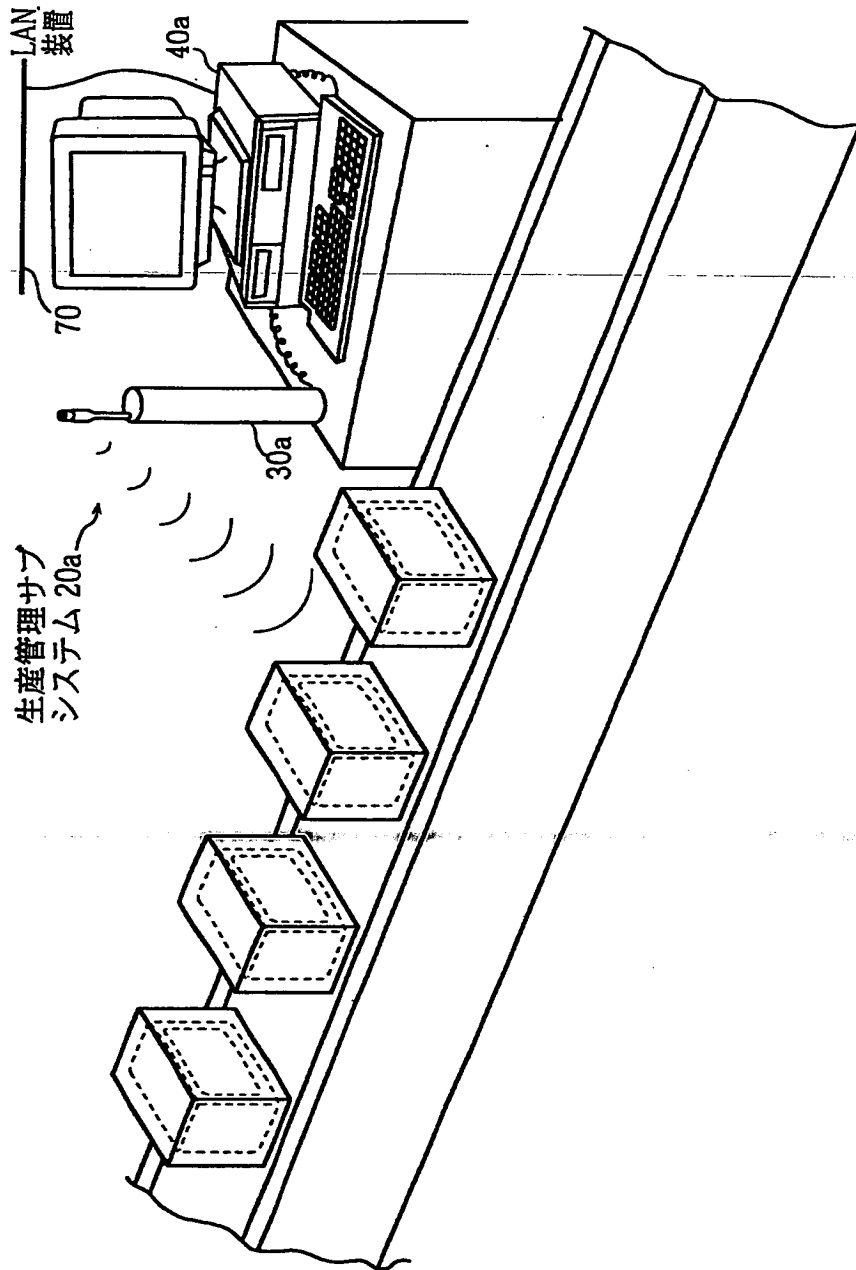
【図 4】



【図 5】

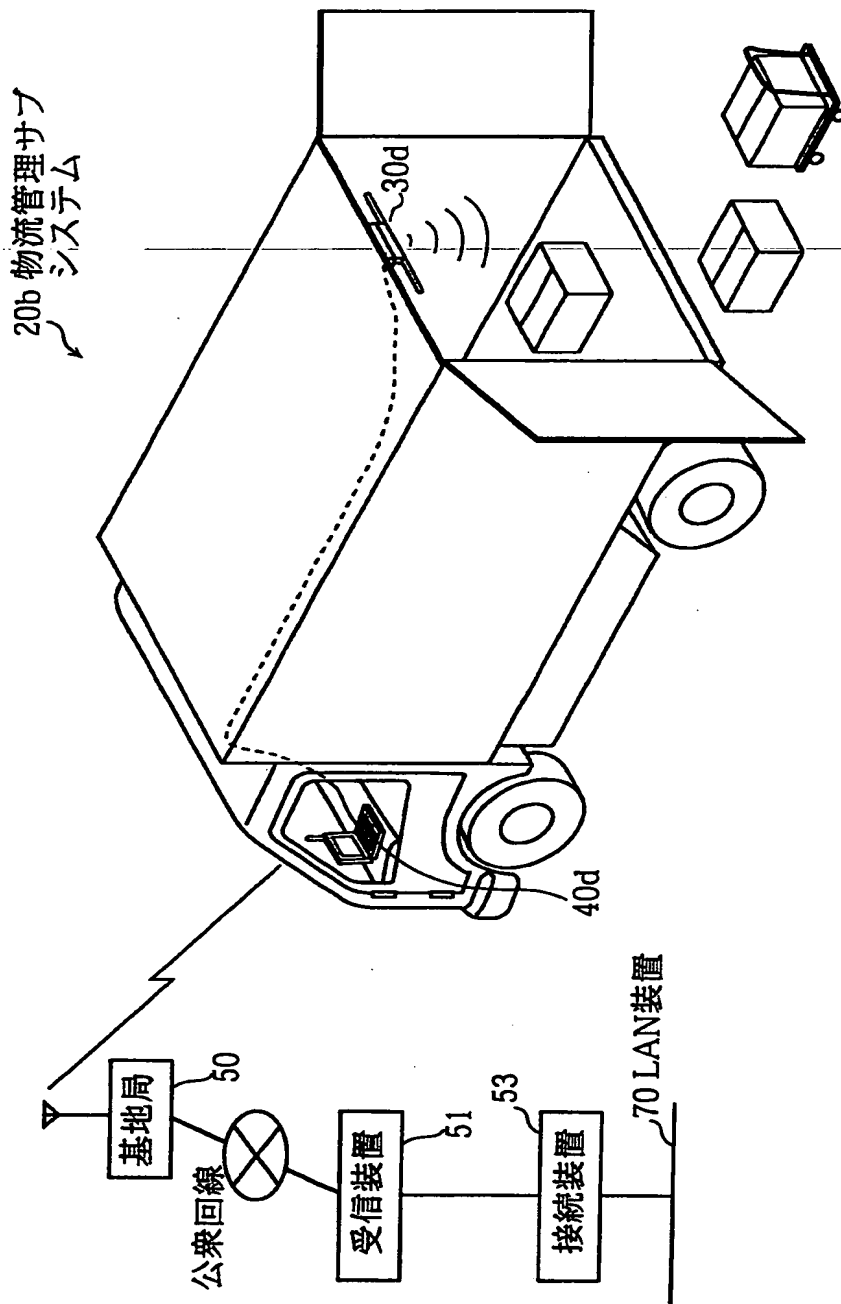


【図 6】

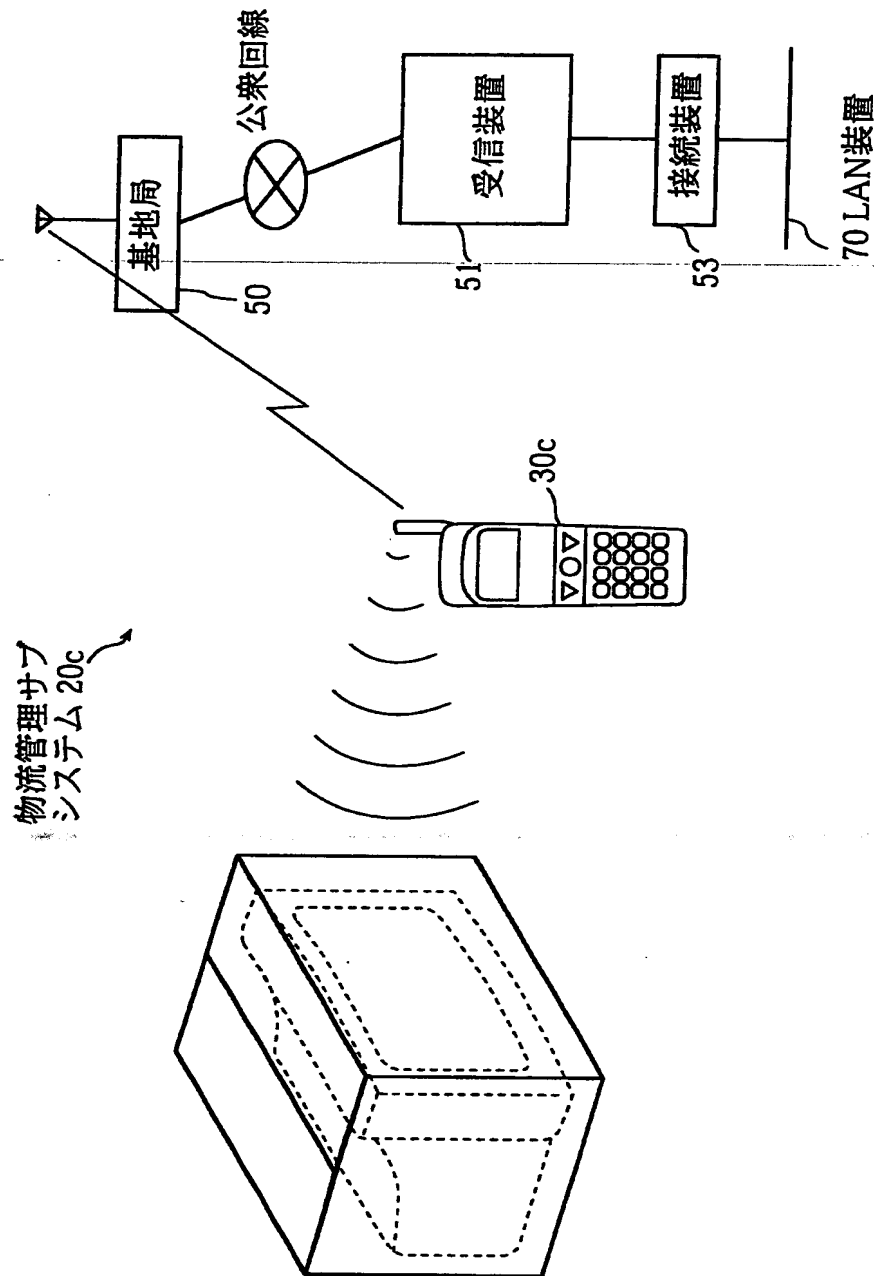




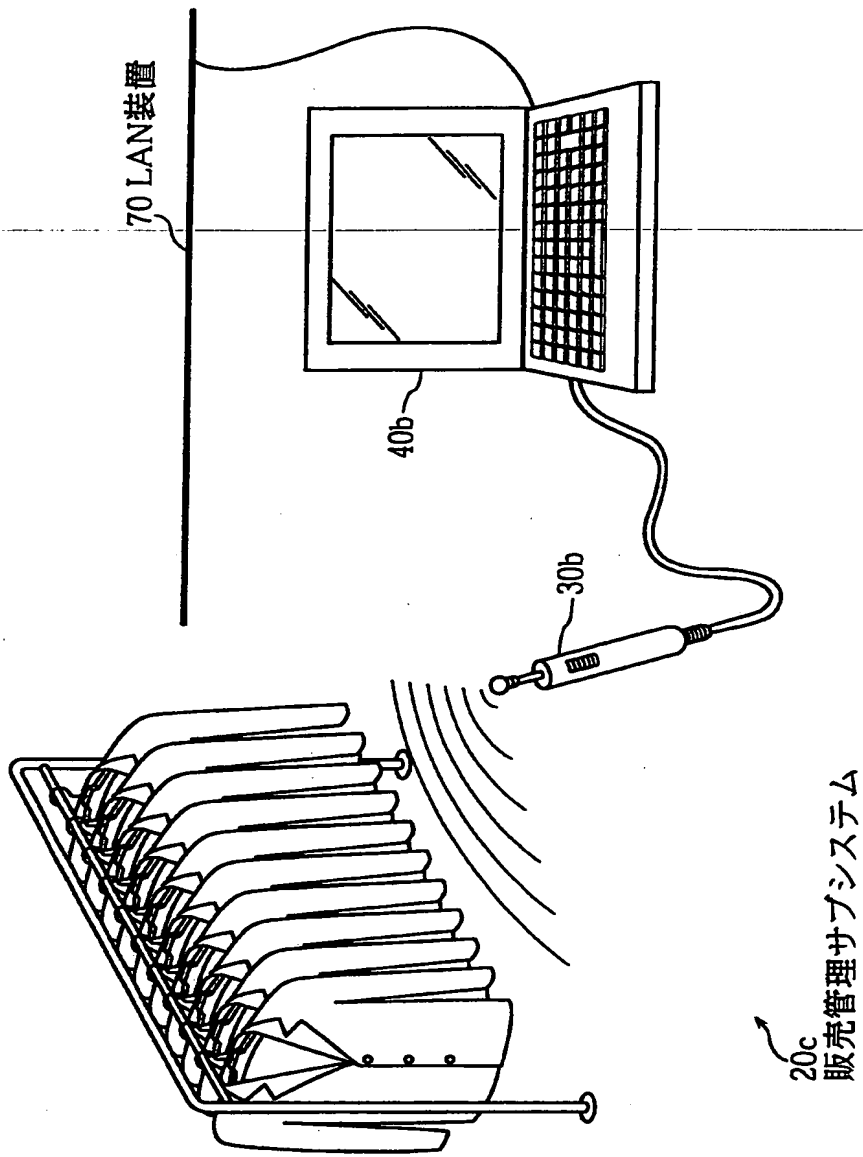
【図 7】



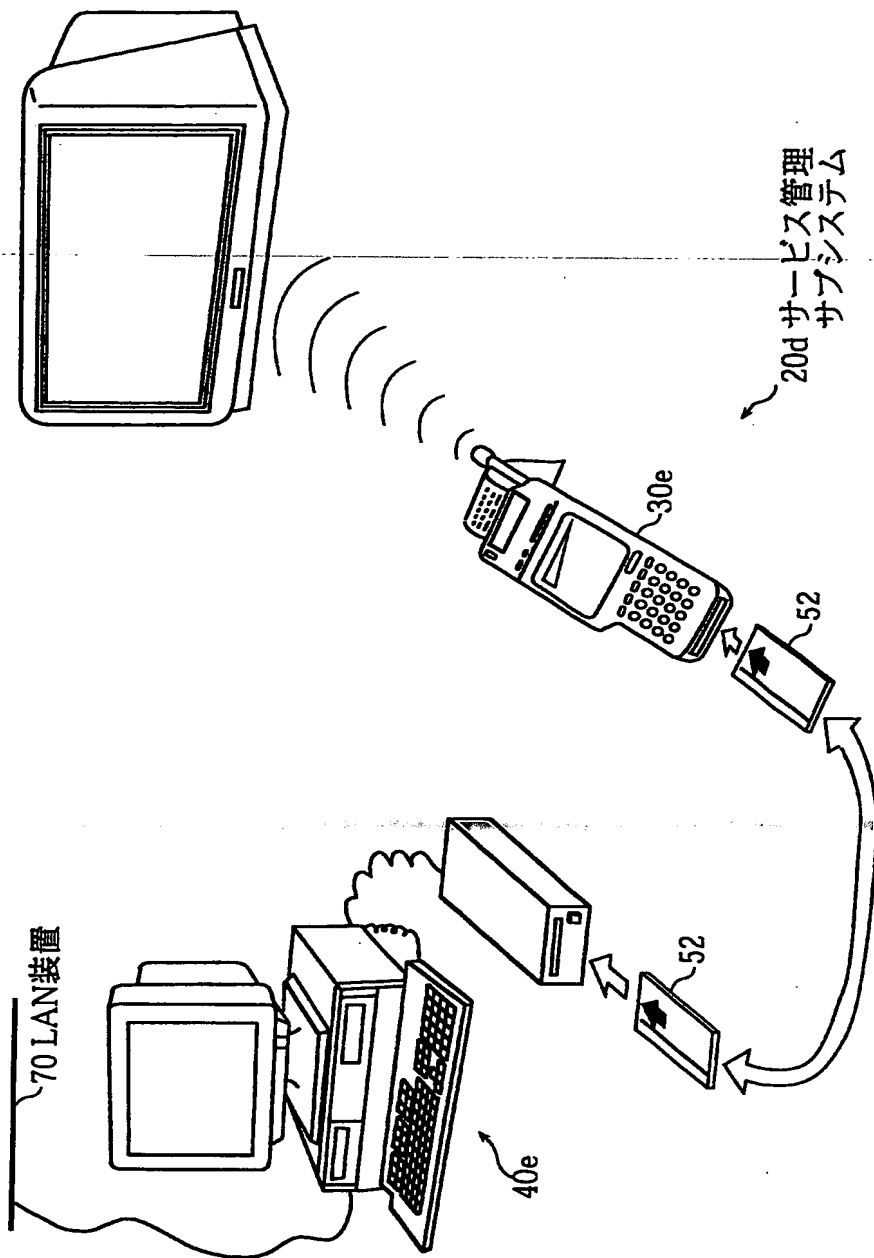
【図8】



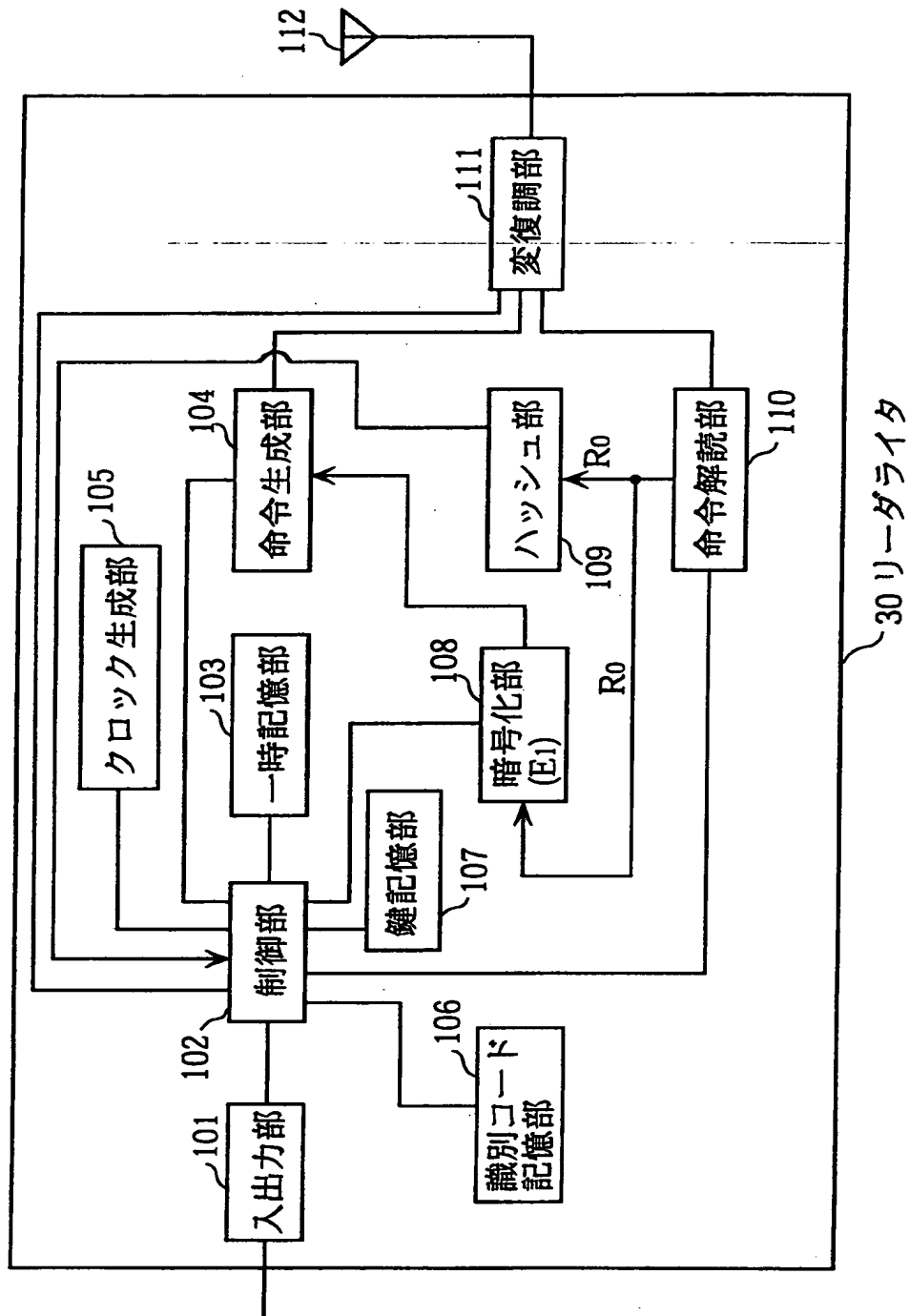
【図9】



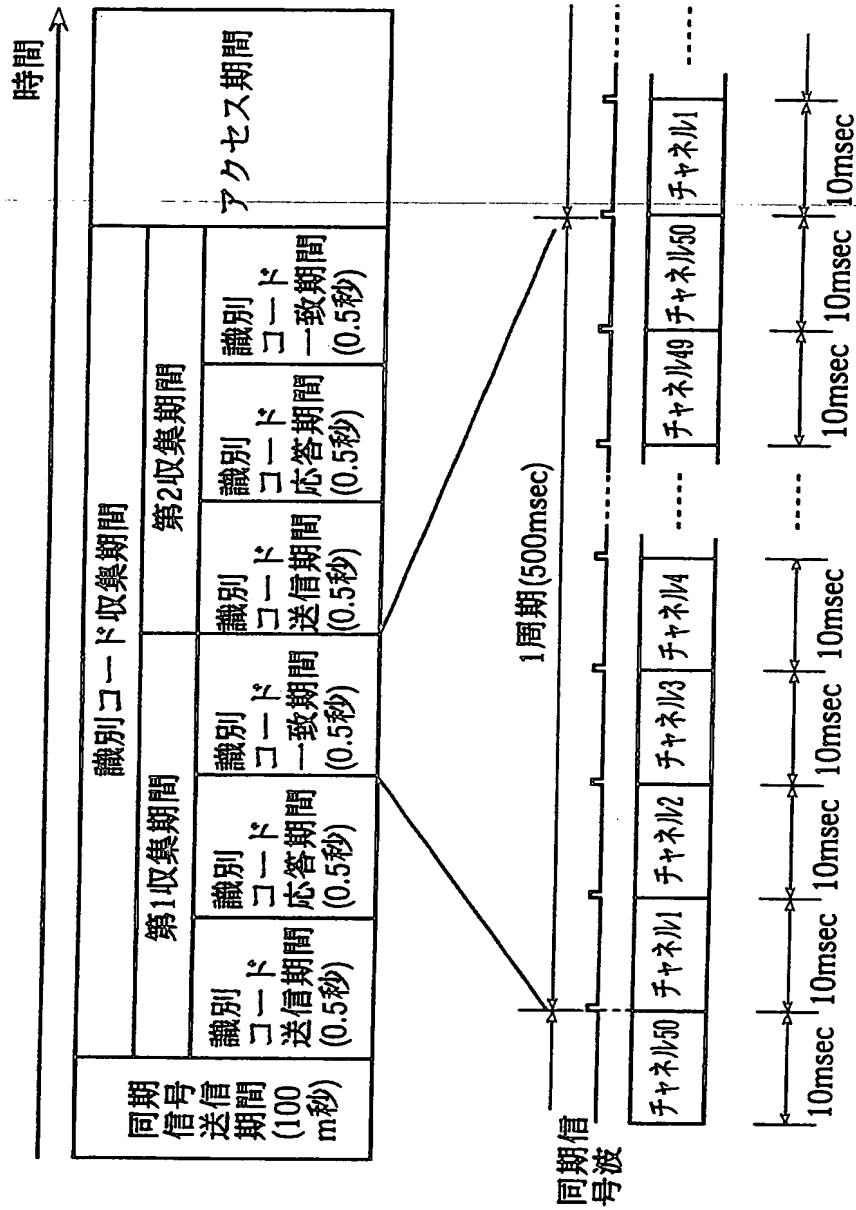
【図10】



【図 11】



【図 12】



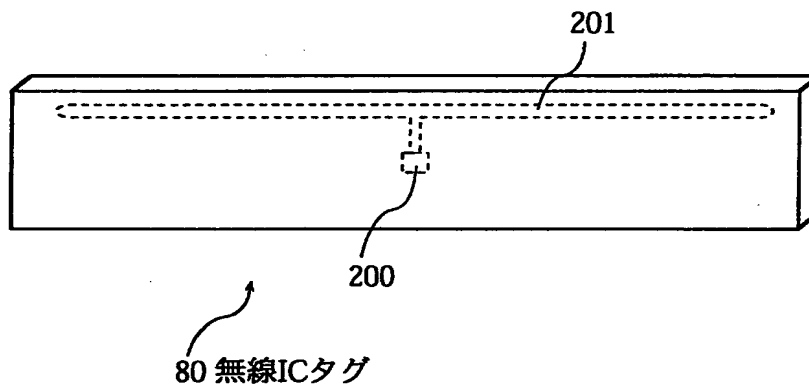
【図 13】

命令種別	オペランド等
同期信号送信命令	同期信号
識別コード収集命令	
アクセス要求命令	識別コード
アクセス命令	
Read 命令	識別コード、物理アドレス、読み出しバイト数
Write 命令	識別コード、物理アドレス、書き込みバイト数、書き込み内容
識別コード応答命令	識別コード
認証子応答命令	識別コード、認証子

【図 1 4】

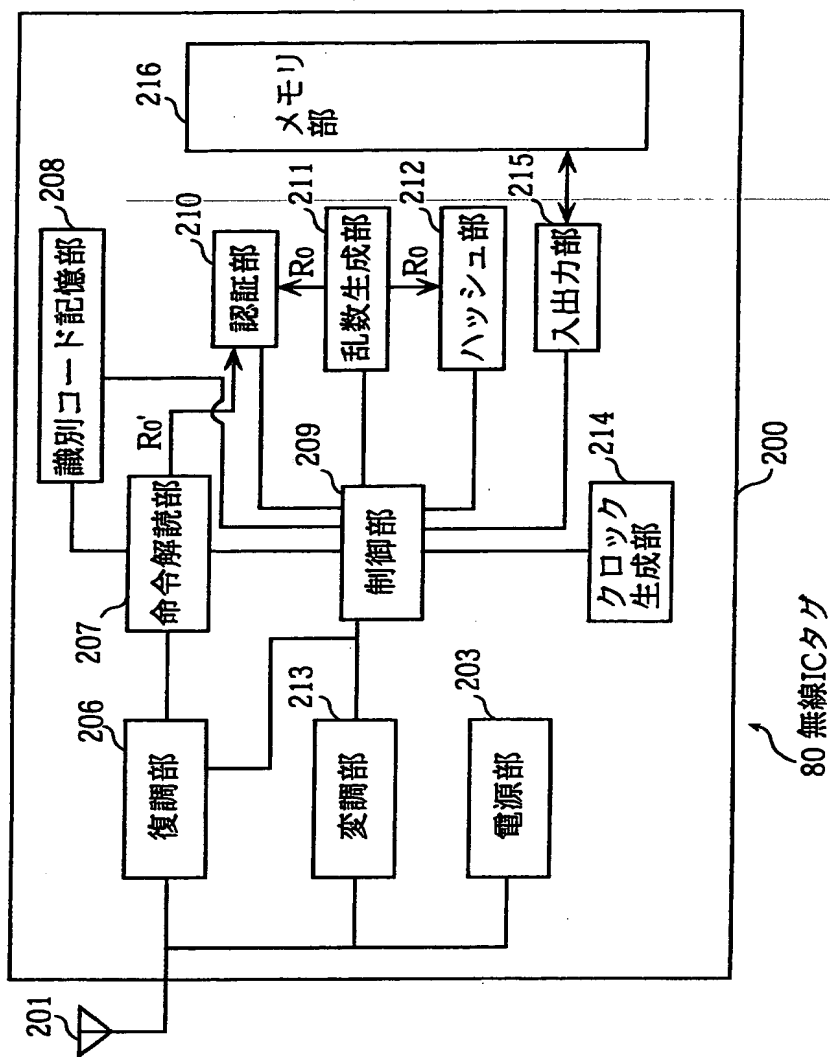
命令種別	オペランド等
識別コード送信命令	乱数R0、識別コード
認証子送信命令	識別コード、認証子
識別コード一致命令	識別コード
アクセス応答命令	識別コード、アクセス応答情報
アクセス不許可命令	識別コード、理由コード

【図 1 5】

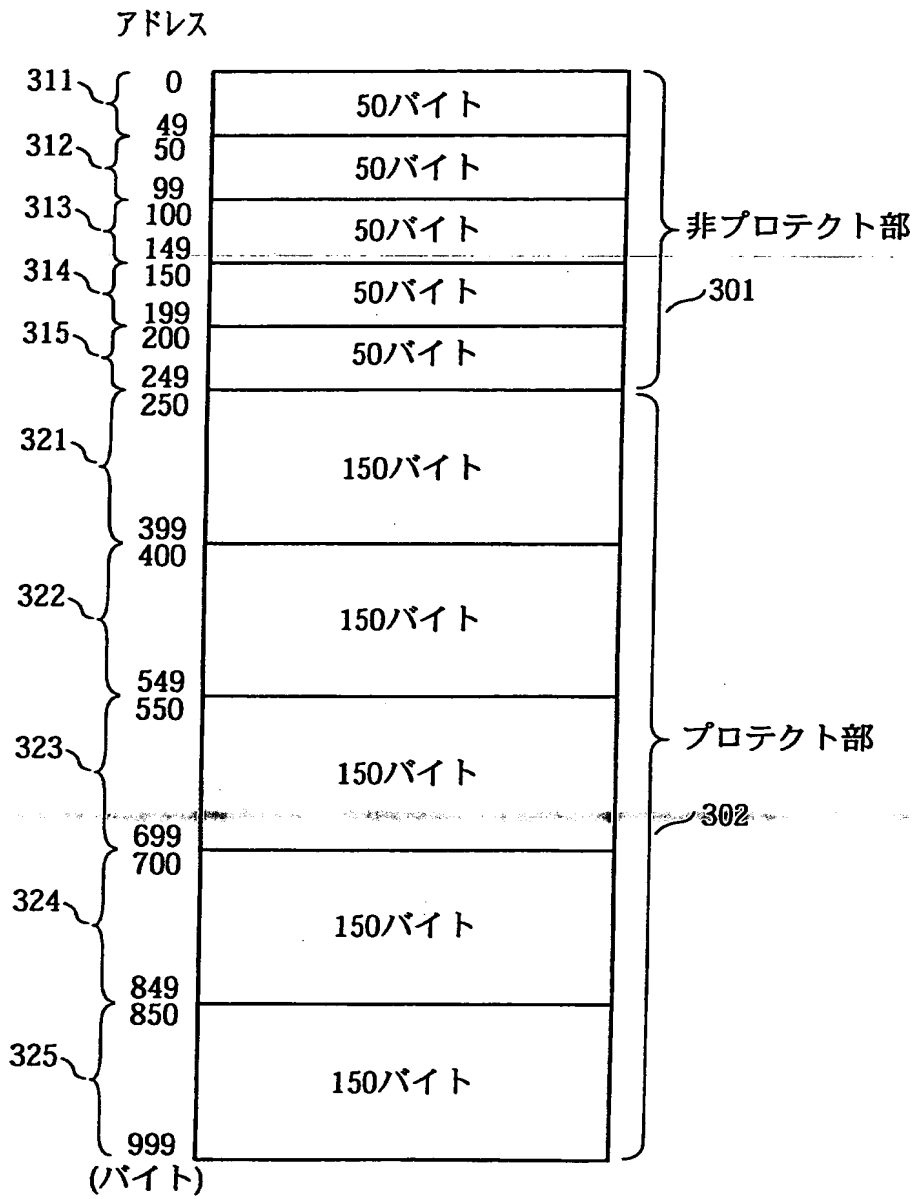




【図16】



【図 1 7】



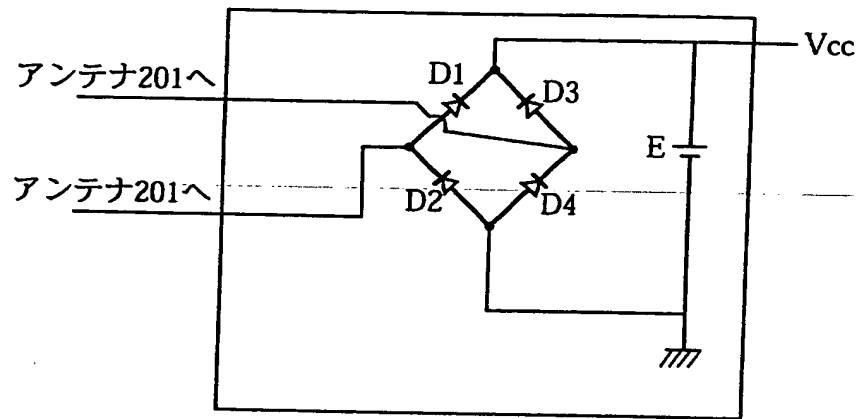
【図 18】

生産ステージ領域				物流ステージ領域		販売ステージ領域		サービスステージ領域		回収リサイクルステージ領域	
非プロ テクト部	メーカー名	運送業者名		保証期間		洗濯方法					
	品名			保証番号							
	品番										
301	製番	入出庫日		卸業者名						回収業者	
	製造日	GLN(グローバル ケージン番号)		小売店名						回収日	
	工場名			販売日						廃棄業者	
プロテクト 部						修理者名		リユース記録			
						修理日					
						修理部品					
302											

ライト  
ワンス部

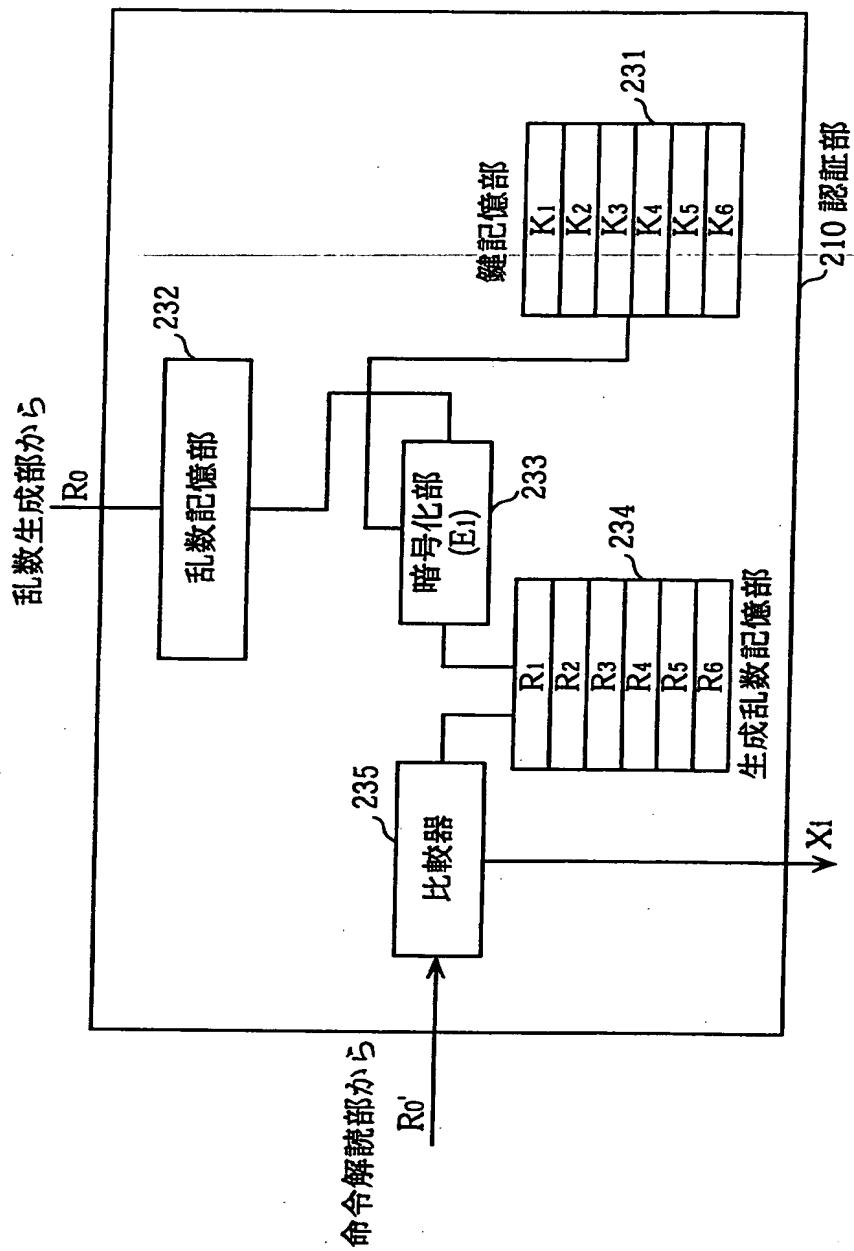
可変部

【図 1 9】

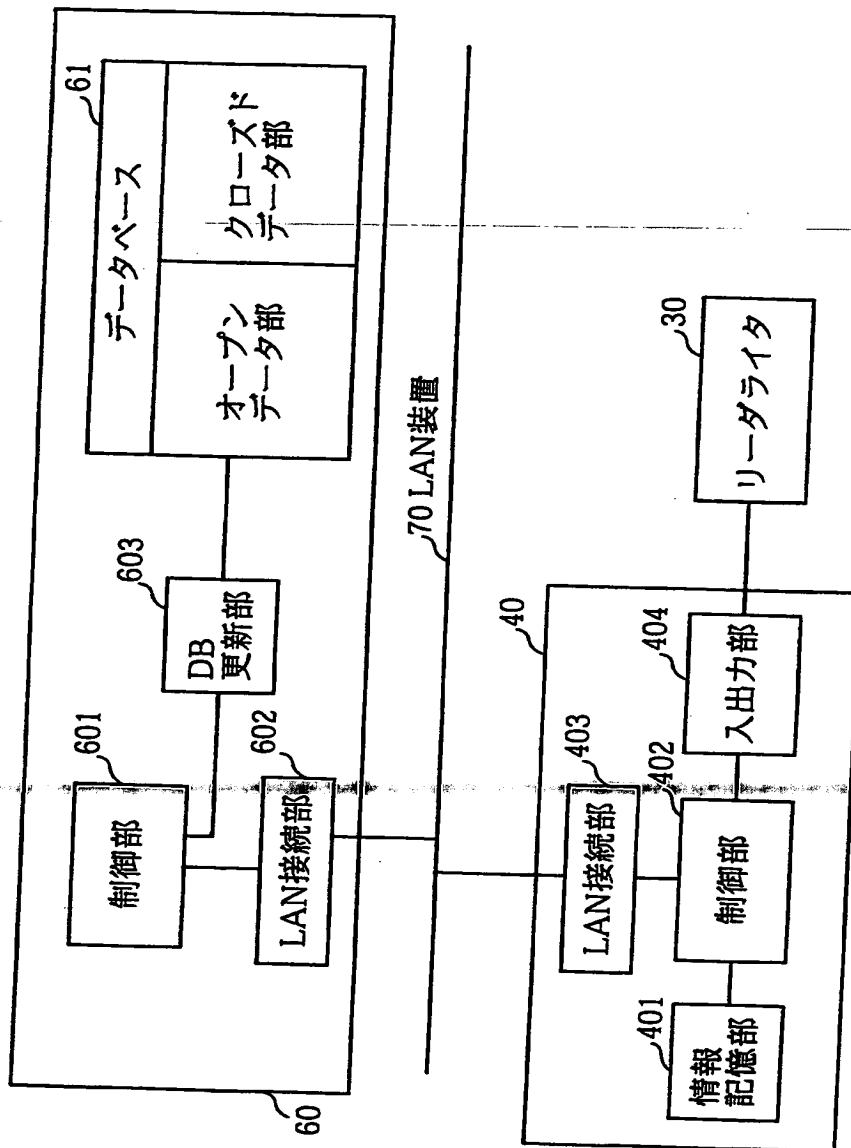


電源回路

【図 20】



【図21】



【図22】

生産データ部	物流データ部	販売データ部	サービスデータ部	回収リサイクルデータ部
--------	--------	--------	----------	-------------

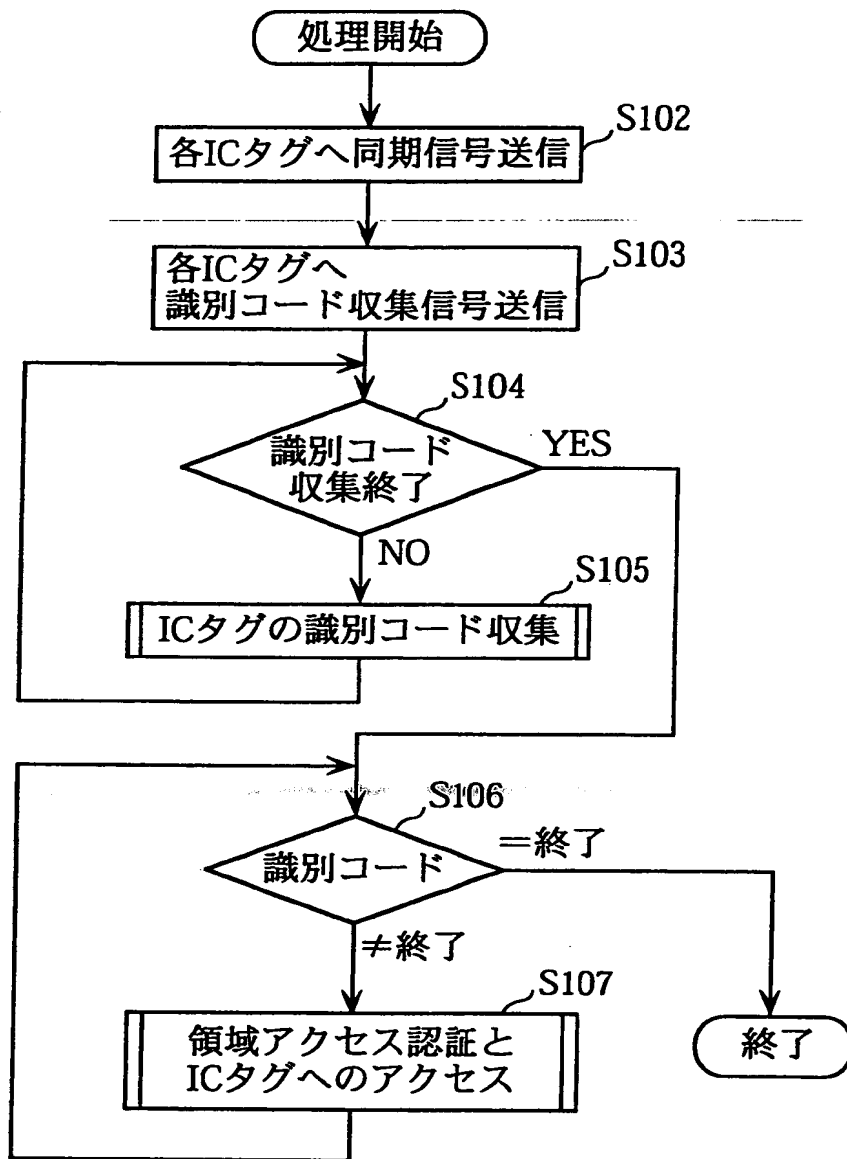
分解方法				リサイクル 活用情報
部品データ				
有毒情報				

オープンデータ部

検査情報	追跡記録	POS情報	品質情報	マニフェスト情報

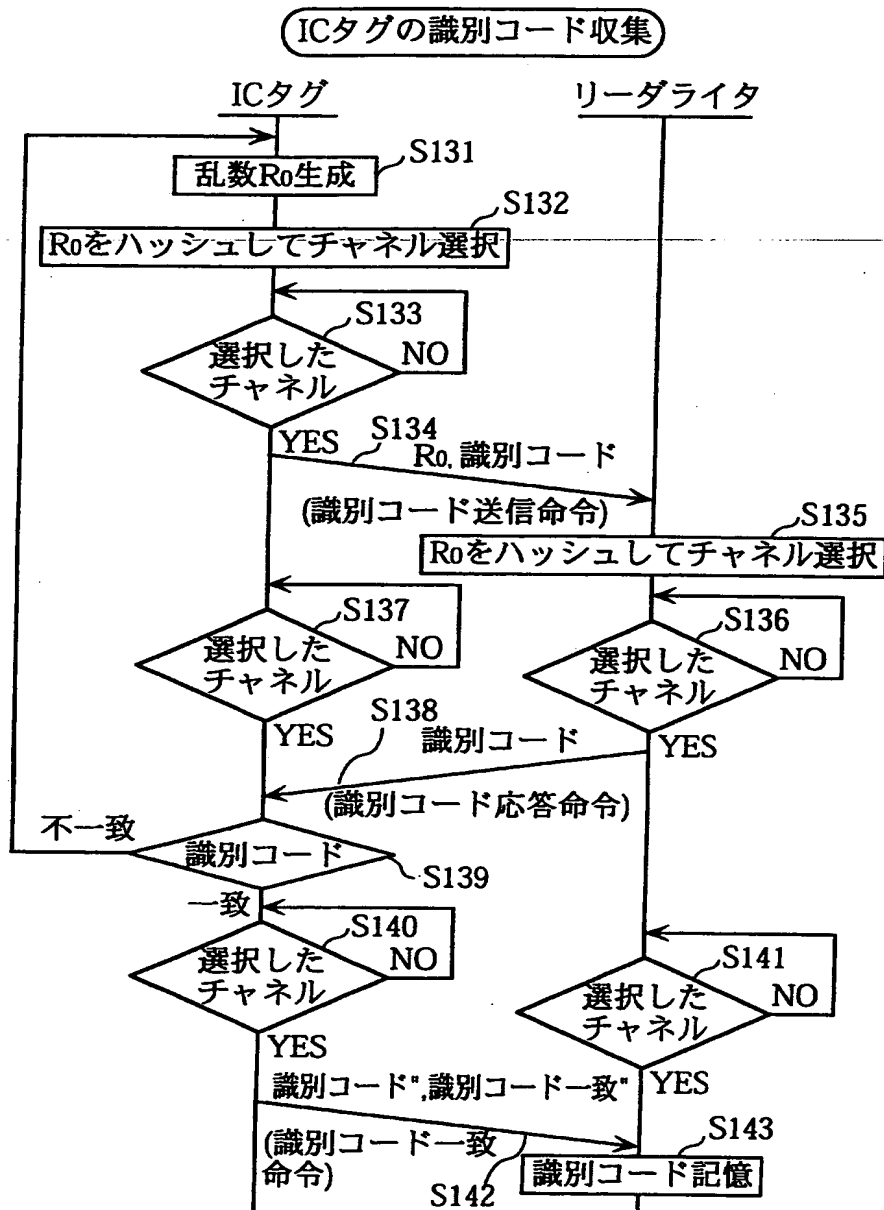
クローズドデータ部

【図 2 3】

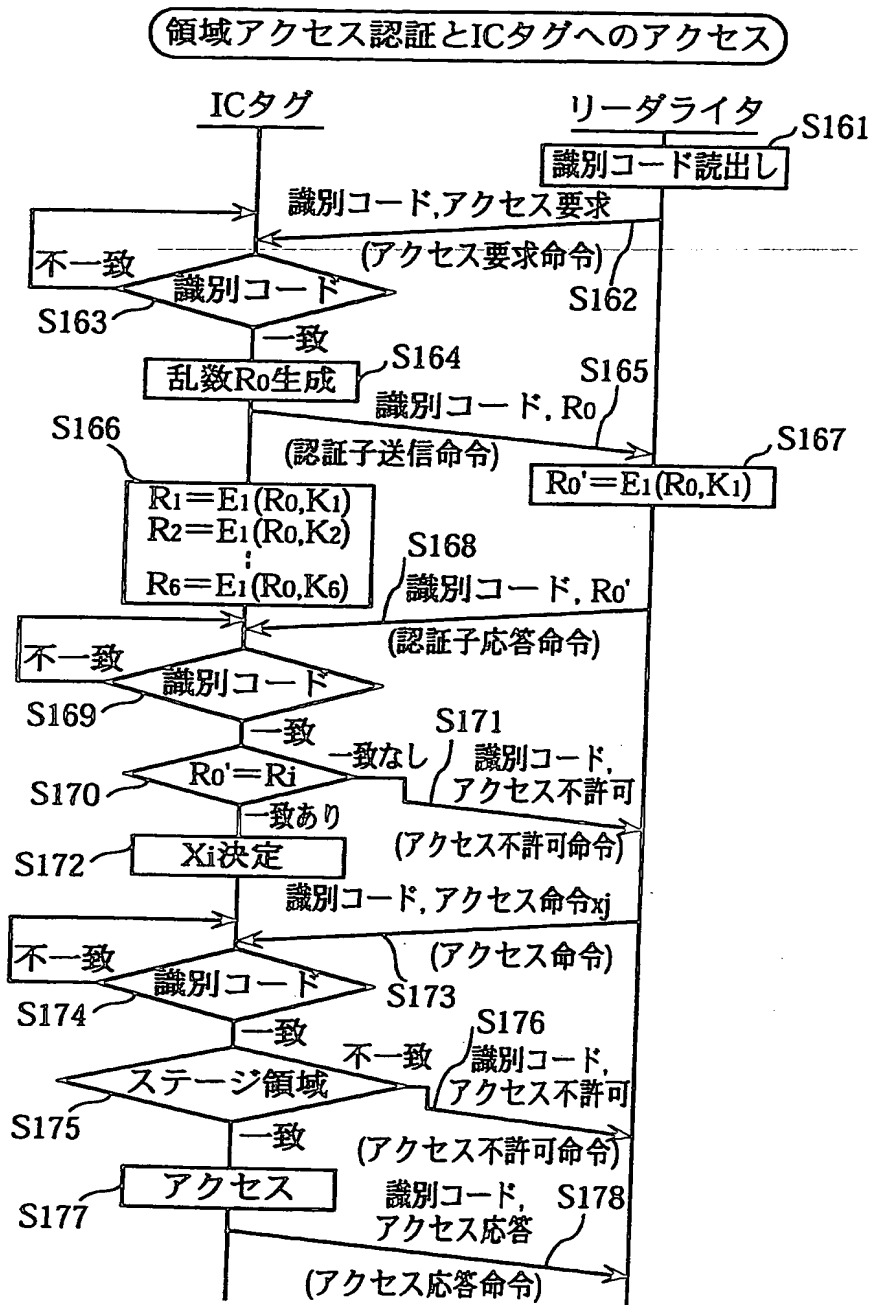




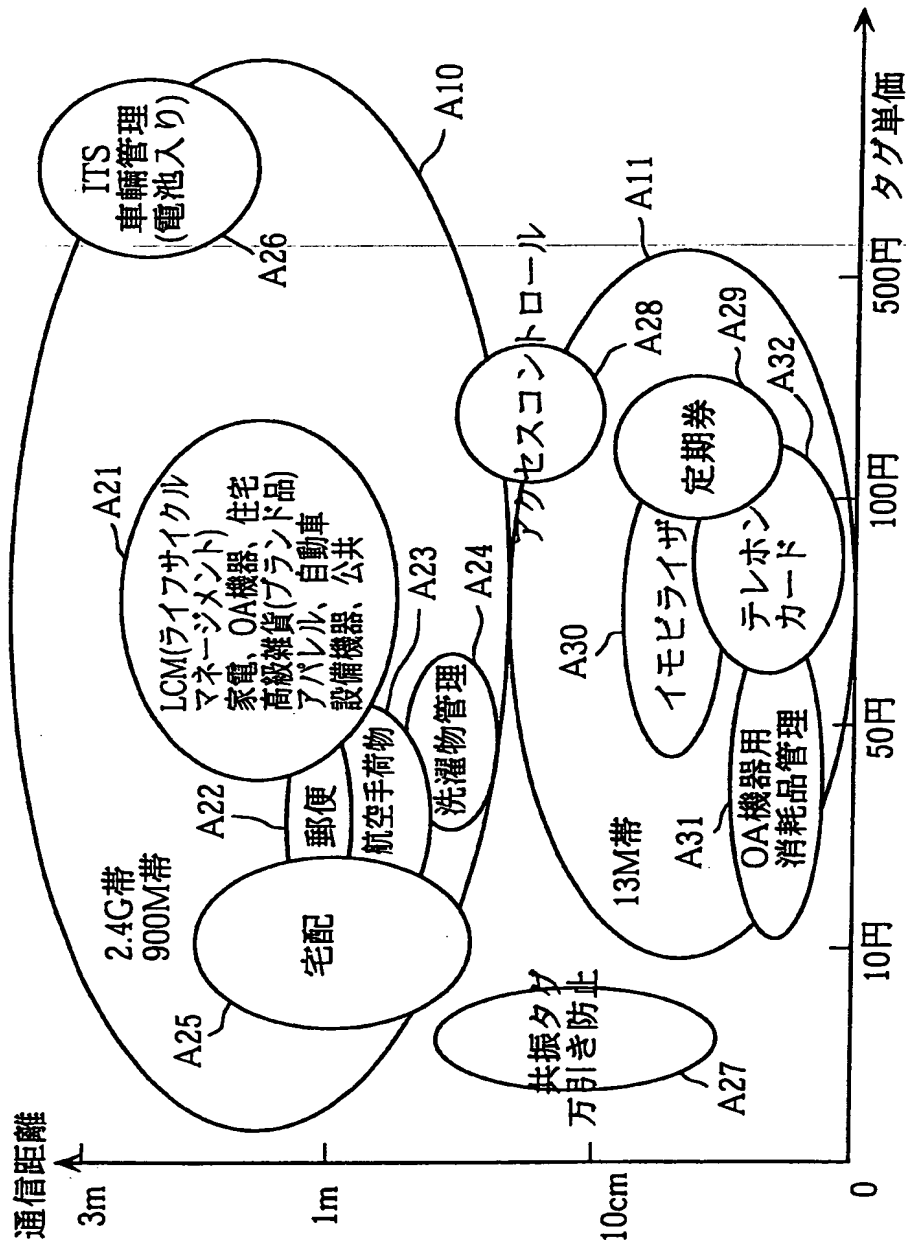
【図 24】



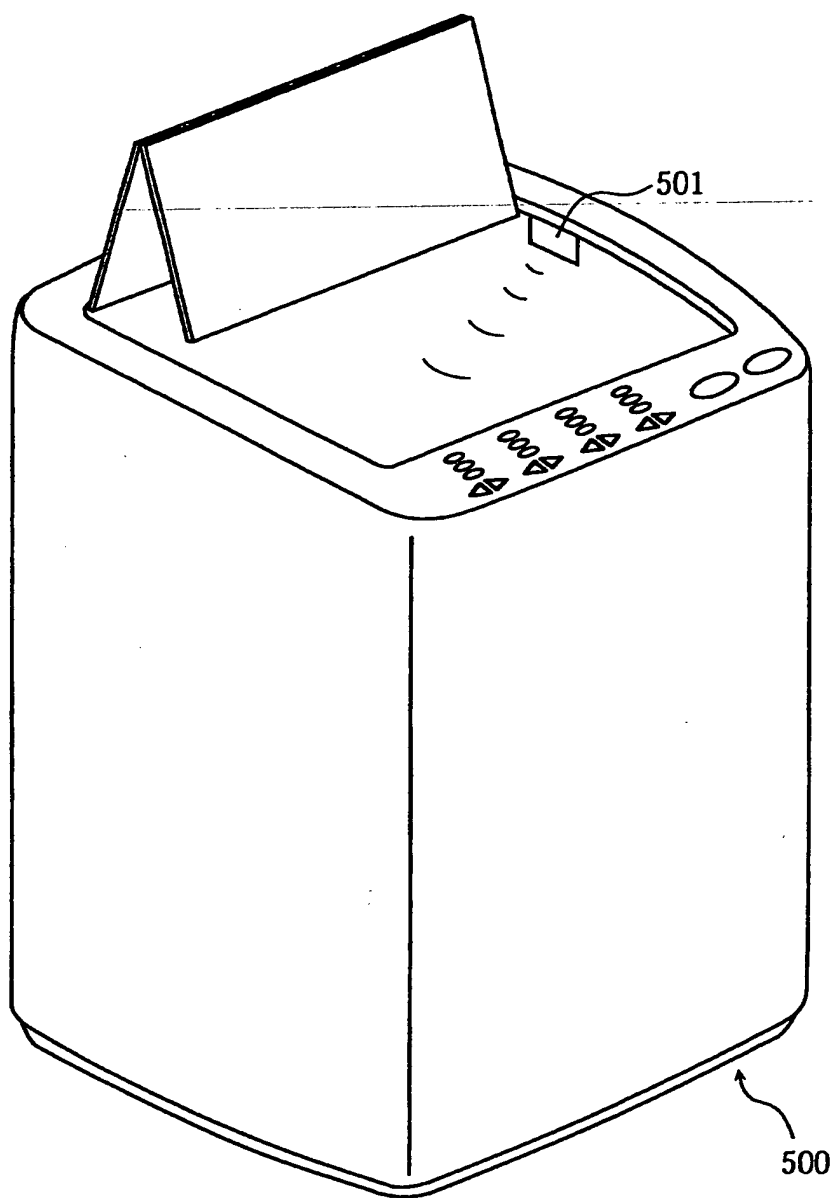
【図 2 5】



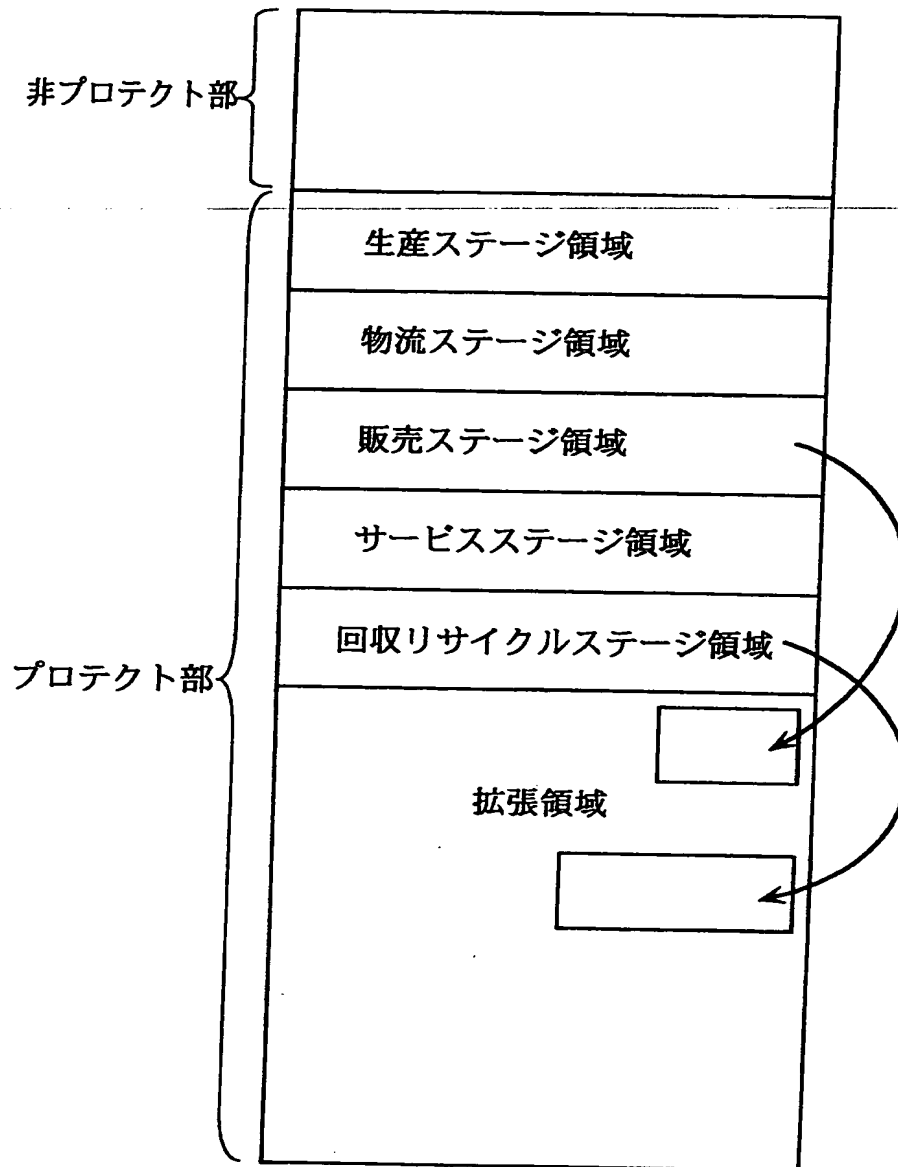
【図26】



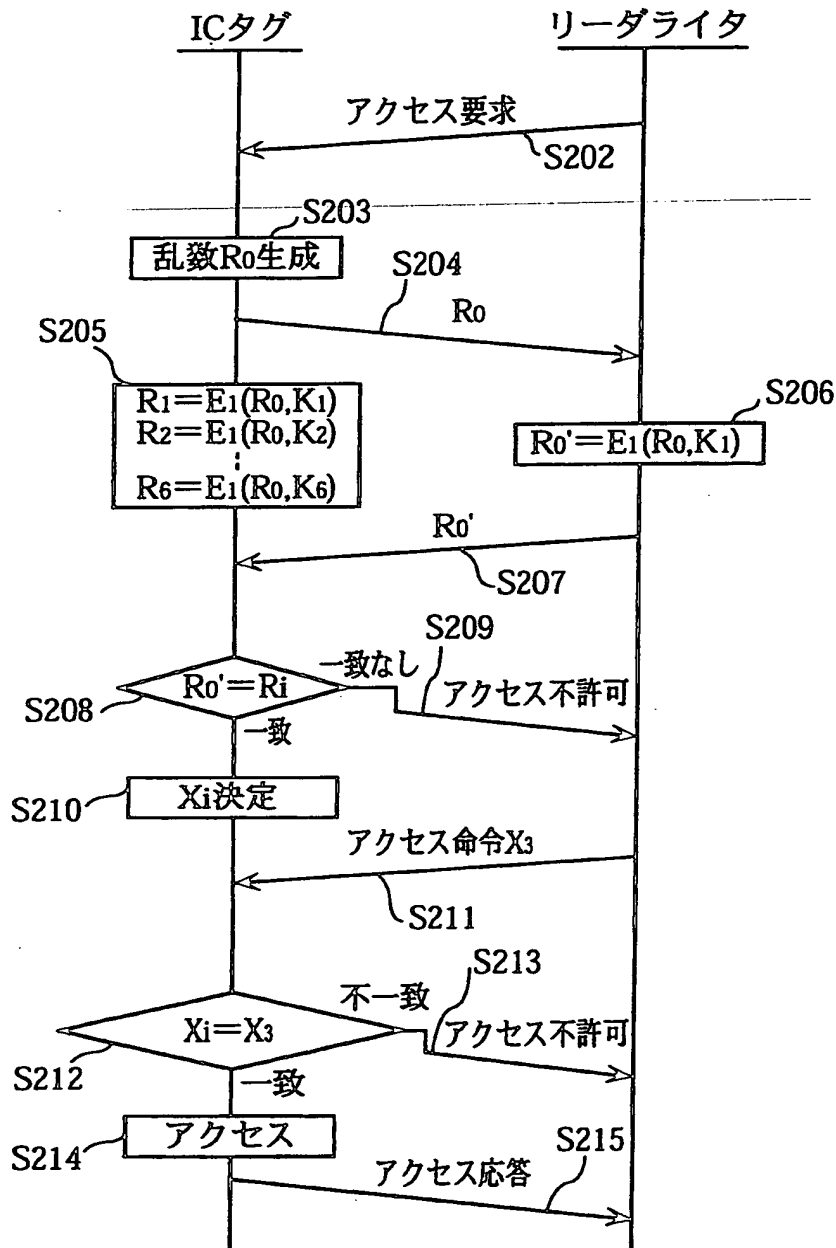
【図 2 7】



【図 28】



【図 29】



【書類名】 要約書

【要約】

【課題】 生産から廃棄に至るまでのライフサイクルにおける複数のステージ毎に秘密の情報を記憶する非接触 I C タグと非接触 I C タグに対してステージ毎に秘密に情報を読み書きできるアクセス装置とを提供する。

【解決手段】 メモリ部は、ステージ数と同数のステージ記憶領域を有し、各ステージ記憶領域は、秘密のステージ識別子により識別され、制御部は、アンテナ部、切換部、インピーダンス切換部、復調部、命令解読部を介して、アクセス識別子をアクセス装置から秘密に受信し、秘密に受信した前記アクセス識別子が前記複数個のステージ記憶領域うちの 1 個のステージ記憶領域を正しく識別するか否かを判断し、正しく識別すると判断される場合に、前記アクセス装置からアクセス情報を受信し、入出力部は、受信したアクセス情報に基づいて、ステージ記憶領域へのアクセスを行う。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号

[000005843]

---

1. 変更年月日	1993年 9月 1日
[変更理由]	住所変更
住 所	大阪府高槻市幸町1番1号
氏 名	松下電子工業株式会社



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

***This Page Blank (uspto)***